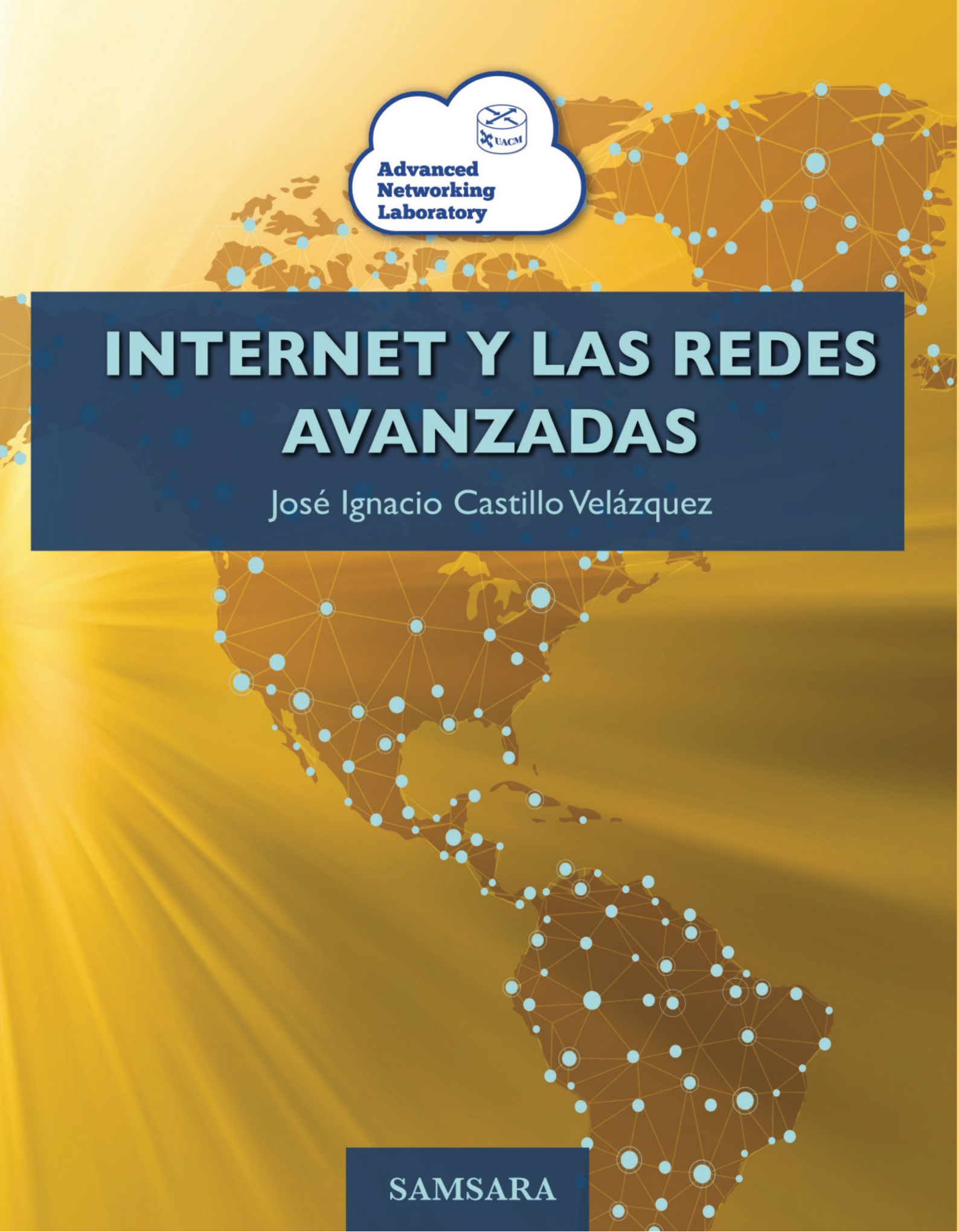


INTERNET Y LAS REDES AVANZADAS

José Ignacio Castillo Velázquez

SAMSARA

Este libro está dirigido a todo estudiante universitario y profesional que desee introducirse a los principios de funcionamiento de los equipos de redes de computadoras e Internet, cubre el área de conocimiento globalmente conocido como "switching and routing" para la tecnología Ethernet. Responde a la pregunta ¿cómo funciona la "¿Internet 1" o comercial, así como la "Internet 2" o las redes avanzadas? La Internet 2 es independiente de la Internet comercial y se usa exclusivamente para investigación y educación, por ello, reciben el nombre de Redes Nacionales para la Educación y la Investigación (National Research and Education Networks - NREN).

Se ofrece un balance entre la teoría y la práctica, cubre los fundamentos teóricos, incluye ejercicios para simulación y emulación, prácticas de laboratorio y evaluaciones para reafirmar los conocimientos y habilidades adquiridas.

EL AUTOR

José Ignacio Castillo Velázquez cuenta con 27 años de experiencia en las TICs, tanto en empresas como en universidades públicas y privadas. Ha participado en 105 proyectos nacionales e internacionales, en las áreas técnicas y de gestión en 17 países.

Como académico cuenta con 50 publicaciones en revistas y congresos arbitrados; 4 libros y 2 reportes técnicos. Ha impartido 135 cursos de licenciatura y posgrado, así como 171 conferencias magistrales en congresos nacionales e internacionales. Es árbitro en revistas y congresos internacionales de IEEE y SPRINGER. Desde 2008 es profesor investigador de tiempo completo en la carrera de Ingeniería en Electrónica y Telecomunicaciones en la Universidad Autónoma de la Ciudad de México (UACM), donde dirige el Advanced Networking Laboratory (ADVNETLAB). Ha laborado en UPAEP, UTM, UAM, UDEFA y BUAP.

Como profesional y consultor ha trabajado en Datacenter Dynamics, RedUno-Telmex, CEDAT-IFE y DICINET y ha escrito 16 reportes técnicos y 2 artículos en telecomunicaciones y Data Centers. Miembro ICREA y de los comités técnicos de IEEE LAN/MAN/cloud computing.

Recibió las distinciones internacionales IEEE Senior Member y IEEE Computer Society Golden Core Member (2011) y Distinguished Lecturer de IEEE Computer Society.

Recibió el premio internacional al mejor artículo en Communications, al mejor artículo en Engineering Education y al mejor artículo en el IEEE ANDESCON 2020. También al mejor artículo en Engineering Education en ANDESCON 2022.

El autor obtuvo sus grados académicos en la Benemérita Universidad Autónoma de Puebla en Puebla, México. Consulte los detalles en https://ignaciocastillo.org/

ISBN 978-607-59377-5-5

9 786075 937755 >

Internet y las redes avanzadas

M. en C. José Ignacio Castillo Velázquez

Universidad Autónoma de la Ciudad de México

2023

Revisores

Dr. Gerardo Laguna Sánchez – UAM – L Edo. Mex.
Dr. Ricardo Marcelín Jiménez – UAM – I - CDMX
Mtro. Pedro Fernando Solares Soto – UIA – CDMX
Dra. Rafaela Blanca Silva López UAM – L - Edo. Mex.
M. en C. Nury Gabriela Ramírez Cely – Continental Automotive - Guadalajara

SAMSARA

2023

Internet y las redes avanzadas
José Ignacio Castillo Velázquez

https://ignaciocastillo.org/

Primera edición, febrero de 2023.

Registro INDAUTOR: 01-2025-043014384800-01

Editor: Sergio A. Santiago Madariaga

maquinahamlet@gmail.com

Corrección de estilo: Dra. Carmen Araceli Eudave Loera

Diseño de portada: Iziar Nancy Eudave Salazar

ISBN 978-607-59377-5-5

Impreso en México

Datos de catalogación bibliográfica: José Ignacio Castillo Velázquez (2023). Internet y las redes avanzadas. México. Ed. Samsara 240 pp.

ÍNDICE

PREFACIO

Este libro está dirigido a todo aquel que desee introducirse a los principios de funcionamiento de los equipos y dispositivos de comunicaciones de datos que dan forma a las actuales redes de computadoras e Internet, tales como los *switches y routers*, con base en la tecnología Ethernet. Será de utilidad para técnicos o profesionistas del área de las tecnologías de la información, que deseen hacer una revisión de los fundamentos de conmutación (*switching) y* enrutamiento *(routing)*.

El libro ofrece un balance entre la teoría y la práctica, pues, además de los fundamentos teóricos, incluye ejercicios para simulación, prácticas de laboratorio y evaluaciones que buscan reafirmar los conocimientos y habilidades adquiridas, así como ayudar a comprender el funcionamiento tanto de la Internet comercial como de la Internet 2 o de las redes avanzadas. Las redes avanzadas son el nombre genérico que reciben las redes de la Internet 2 en cada país. La Internet 2 es independiente de la Internet comercial y se usa exclusivamente para investigación y educación, por ello, también reciben el nombre de Redes Nacionales para la Educación y la Investigación (*National Research and Education Networks* - NREN).

- **Organización del libro**

El libro consta de cuatro partes, las cuales están estructuradas de manera secuencial con base en la construcción del conocimiento y su complejidad. Las tres primeras partes pueden usarse para un curso de nivel licenciatura y la cuarta para un curso de posgrado.

- **Texto para curso de pregrado**

Como punto de partida, se espera que el lector cuente con conocimientos básicos de redes de datos, como el modelo ISO/OSI y el modelo TCP/IP y de preferencia el modelo cliente servidor, por lo que, para apoyar al lector para identificar sus conocimientos previos, se incluye una evaluación diagnóstica. También recomiendo, que, de tener dudas, se consulte el libro ***Redes de datos: Contexto y evolución,* 3ª ed., 2019**, de mi autoría. Las tres primeras partes cubren el curso de licenciatura conocido globalmente en el área de redes y telecomunicaciones, como "***switching and routing"*** correspondiente a la tecnología "Ethernet", la tecnología que venció a tecnologías como ATM, X.25, Apple Talk, etc., por su simplicidad, eficiencia y economía. En este libro profundizaremos en el estudio de las capas 1, 2 y 3 de los modelos ISO/OSI Y TCP/IP.

La primera parte del libro, titulada "Ethernet LAN", se compone de los capítulos I y II. El capítulo I: "Tecnologías de legado", abarca las tecnologías de transición de la conmutación de circuitos a la conmutación de paquetes, así como la tecnología de los *hubs,* e incluye la práctica de laboratorio 1: "Red LAN con base en *hubs*" (tiempo sugerido para el capítulo: 6 horas). Mientras

que en el capítulo II se aborda la "conmutación (*switching*) en LAN"; cubre la práctica de laboratorio 2: "LAN con base en switch" y la práctica 3: "Subredes vía NIC y vía switch" (tiempo sugerido para el capítulo: 12 horas).

La segunda parte del libro, titulada "enrutamiento", se conforma de los capítulos III y IV. El capítulo III: "Enrutamiento estático", aborda los fundamentos de enrutamiento (*routing*) del tipo estático, se revisa brevemente la expansión de las tecnologías Ethernet, así como la infraestructura de red y se incluye la práctica de laboratorio 4: "Enrutamiento estático" (tiempo sugerido para el capítulo: 12 horas). El capítulo IV: "Enrutamiento dinámico", aborda el enrutamiento de tipo dinámico, el cual usa los protocolos de enrutamiento interior *Routing Information Protocol* (RIP) y *Open Shortest Path First* (OSPF) e incluye la práctica 5: "Enrutamiento dinámico RIP y OSPF" (tiempo sugerido para el capítulo: 18 horas).

La tercera parte del libro, "Infraestructura y gestión de red", se conforma de los capítulos V y VI. El capítulo V: "Infraestructura de red", aborda los equipos y topologías que dan soporte a redes LAN, MAN, WAN y estándares básicos para centros de datos e incluye la práctica 6 "Infraestructura" (tiempo sugerido para el capítulo: 12 horas). El capítulo VI: "Gestión de red", para lo cual se aborda el protocolo de gestión *Simple Network Management Protocol* (SNMP), incluye la práctica 7 "Gestión" (tiempo sugerido para el capítulo: 18 horas).

El objetivo del curso, de casi 80 horas, es que el estudiante haya adquirido los conocimientos y haya desarrollado las habilidades necesarias para monitorear, configurar y resolver problemas al realizar la conectividad y gestión de redes LAN y MAN bajo el conjunto de protocolos IPv4, habiendo cubierto los 3 primeros niveles de pensamiento inferior y los dos primeros niveles de pensamiento superior de la taxonomía de Bloom.

- **Texto para curso de posgrado**

La cuarta parte, "Redes avanzadas" se conforma de los capítulos VII y VIII. El capítulo VII, "Introducción a las redes avanzadas", aborda las principales redes de Internet 2 en el mundo, centrándose en su topología de *backbone* (dorsal o núcleo), considerando al protocolo de enrutamiento *Border Gateway Protocol* (BGP), mismo que permite interconectar a los sistemas autónomos; incluye la práctica 8 "Redes avanzadas" (tiempo sugerido para el capítulo: 20 horas). El capítulo VIII "Protocolo IPv6" aborda las limitaciones de IPv4, indica cómo pueden convivir ambos protocolos, y aborda los detalles del protocolo IPv6, usado actualmente por todo proveedor de servicios de Internet (comercial o no comercial) en su nivel de *backbone,* incluye la práctica 9 "IPv4 vs IPv6" (tiempo sugerido para el capítulo: 20 horas).

El objetivo del curso, de casi 40 horas, es que el estudiante haya obtenido los conocimientos y haya desarrollado las habilidades necesarias para monitorear, configurar y resolver problemas al realizar la conectividad y gestión de redes LAN, MAN y WAN bajo el conjunto de protocolos IPv6, habiendo cubierto los 3 primeros niveles de pensamiento inferior y los dos primeros niveles de pensamiento superior de la taxonomía de Bloom.

- **Metodologías de enseñanza y estrategias de evaluación del aprendizaje.**

Se espera que el profesor que imparta el o los cursos asociados a este libro use al menos como metodologías de enseñanza, además de la **clase magistral**, el **aprendizaje con base en la resolución de problemas** y la del **uso de simuladores** y de equipos de **laboratorio,** como se indica en las prácticas de laboratorio, pero también el de **casos de estudio** y el **aprendizaje con base en proyectos**.

En cuanto a las estrategias de evaluación de los aprendizajes se recomiendan al menos cuatro: la **entrega de tareas**, la **participación en laboratorios,** el **reporte de prácticas de laboratorio y** las **evaluaciones,** tanto diagnóstica como formativas.

- **El laboratorio ADVNETLAB y sus productos como apoyo.**

Si tomas cursos en la carrera de Ingeniería Electrónica y Telecomunicaciones o Ingeniería de Software en la UACM puedes contar con el laboratorio de redes avanzadas (**Adv**anced **Net**working **Lab**oratory - ADVNETLAB), para el desarrollo de proyectos, y con el Seminario ADVNETLAB el cual toca diversos temas de actualidad relacionados principalmente con las TICS, pudiéndose abordar en español o inglés. Tanto el laboratorio como el Seminario ADVNETLAB se fundaron en enero de 2013 en la UACM campus San Lorenzo Tezonco (SLT).

En estos 10 años, como parte de nuestros productos están nuestros 17 ingenieros titulados desde 2015 a 2022: 14 egresaron de la UACM de México, y 3 de la UNAS de Perú, y se han diplomado 3 ingenieros en redes corporativas. También se han generado 38 publicaciones, de ellas 34 están indexadas a SCOPUS, 32 como *conference papers* y 2 como *journal papers* JCR, ambas en el cuartil Q4.

Adicionalmente se desarrolló y registró ante Indautor el software de gestión de eventos y conferencias UTILCON (http://utilcon.esy.es/). Nuestra huella de colaboración se ha dado con 4 universidades, en orden cronológico: la UNAS en Perú, la UPM en España, la UPS en Ecuador y la UAM en México. También tenemos relación con empresas y asociaciones, las cuales organizan eventos dentro del ámbito de la industria de las TICS, a las que pueden acceder nuestros tesistas de licenciatura.

- **Habilitación para la profesión de telecomunicaciones y su campo laboral.**

Al concluir satisfactoriamente esta obra, el estudiante deberá haber desarrollado conocimientos y habilidades que le permitan su integración en el mercado laboral de las tecnologías de la información y las comunicaciones como administrador de redes LAN y MAN, con el curso de licenciatura y WAN con el curso de posgrado.

Desde 1990, cuando apareció la Internet en México, hasta 2022, los administradores de redes recién egresados obtienen ingresos superiores a la media nacional para profesionistas en México de acuerdo con el INEGI y los observatorios laborales, el cual es aproximadamente $12,900 mensuales (678 USD). Mientras que el ingreso mensual en compañías internacionales de telecomunicaciones no mexicanas es superior y se incrementa cuando se pasa de los niveles *Junior* a *Senior* o a niveles de mandos medios, gerenciales o directivos que permiten ingresos de alrededor de los $120,000 (6,315 USD). Si bien este ingreso no coloca a una persona en la llamada clase alta a la que pertenece el 1.7% de la población, sí la coloca dentro de la clase media a la que pertenece el 39.1% de la población mexicana en 2022.

- **El idioma inglés en la formación de un ingeniero**

Desde el 2000, no pocas veces he escuchado opiniones en el medio académico, tanto de estudiantes de ciencias e ingeniería, así como profesionistas egresados, ya en el sector industrial, que cuestionan varios de los cursos que toman o tomaron durante su formación profesional, considerándolos poco atractivos, insuficientes o poco útiles. Tales opiniones, nos indican un sentido altamente pragmático o utilitarista de lo inmediato y no del mediano, ni largo plazo, pero también nos indican una falta de formación sistémica, quizás alentadas por el sistema educativo imperante en México y en nuestro mundo altamente globalizado. Cuando pensamos en avances científicos y tecnológicos pensamos en China e India, países con el mayor crecimiento desde el año 2000, y nos encontramos que tal ascenso se ha debido a muchos factores, entre ellos muchas políticas proteccionistas, el crecimiento interno y el trabajo, que les permitió elevar su desarrollo, indicado por su Producto Interno Bruto. En términos tecnológicos, Japón, en la década de los 60, copiaba y exportaba malos productos; en los años 70, había igualado a los mejores productores de tecnología y, en los 80, ya era el referente mundial en tecnología; ello le llevó a ser en la década de los 90 la segunda economía global. Para ello tuvieron que comunicarse en inglés. El mismo patrón siguieron China e India, preparándose, desde las décadas de 1980 y 1990, identificando y copiando al mejor. Al principio de este siglo muchos de sus productos eran de mala calidad o de calidad aceptable. China se convirtió en la “fábrica del mundo” gracias a los mecanismos impulsados por

su gobierno en áreas estratégicas de ciencia y tecnología, sustituyendo así la importación por el desarrollo de sus propios equipos científicos y tecnológicos, e incluso exportándolos. Mientras que, por ejemplo, en EUA de 1990 a 2003 la producción científica exclusivamente de científicos estadounidenses se mantuvo sin crecimiento y su producción compartida se redujo de 38% al 30%. En 2005, EUA alcanzó la misma desigualdad que en 1929 (la gran depresión) y el Reino Unido se colocó como el país europeo con mayor desigualdad. La crisis de 2008 fue una oportunidad para China y, para 2010, sus productos eran buenos y año con año desplazaban a las potencias occidentales en uno o varios rubros. Finalmente, para 2016 China ya había superado a los EUA, al producir la mayor cantidad de publicaciones científicas.

En China e India el aprendizaje del idioma inglés, el idioma de la ciencia y la tecnología fue factor clave para las 4 revoluciones industriales, empoderándole para la transferencia y desarrollo tecnológico que le ha permitido reducir el gradualmente subdesarrollo. Pese a que la India fue colonia inglesa, solo el 10% de su población habla el idioma inglés y tienen como frase generalizada "*English, easy to learn difficult to master*". La comunicación en el idioma inglés es una condición necesaria para tener una carrera exitosa, tanto en el ámbito académico como de la industria, para comunicar ideas con colegas de todo el mundo, pero en el ámbito de ciencia y tecnología principalmente. Los colegas asiáticos no tienen los pausados acentos británicos o estadounidenses, ellos a nadie van a esperar.

En 2021, la UNESCO, órgano de la ONU, integrada por 193 países, reportó que, a nivel mundial, somos 8.8 millones de profesores-investigadores de tiempo completo, de ellos el 25% son de China y EUA, según reporta cada país. De ellos, sólo los países del G20, casi el 10%, generan el 88.8% de la producción científica mundial, prácticamente en inglés: Brasil aporta el 2.1%, México el 0.6% y Argentina el 0.4%. Por ejemplo, en 2019 las publicaciones en SCOPUS se dieron así: Brasil 74,270; México 23,508; y Argentina 12,280. Esto es producto de la inversión del PIB, pero también de políticas de adopción del idioma inglés, las cuales Brasil ha venido implementando desde la década de los años 80 en ciencia y tecnología. Sin ir muy lejos, en el pasado IEEE CCECE (*Canadian Conference on Electrical and Computer Engineering*) 2020, realizado en Canadá, con publicaciones SCOPUS en inglés, de 160 aceptados y publicados, solo hubo 9 artículos de Brasil por las "*University of Campinas*", "*Federal University of Goiás*" y "*Polytechnic School University of S. Paulo*", y 2 artículos de México, por la UACM-ADVNETLAB.

Por su parte, el *AD Scientific Index* 2022 tiene un registro de más de un millón de científicos activos, de 216 países repartidos entre casi 19,000 universidades en el mundo. En México encontramos 12,455 científicos de 352 universidades o instituciones de educación superior.

Mientras que, del lado de la industria, de acuerdo con el IMD *World Competitiveness Ranking* 2020, España se encuentra en la posición 36, México en la 55 y Brasil en la 59, entre 63 países. Por las razones indicadas, si bien este libro está escrito en español, se mantienen los anglicismos tecnológicos que rigen el argot en las esferas donde se desarrolla la ciencia, la tecnología, el desarrollo y la transferencia tecnológica y la innovación. Además, la experiencia nos deja claro que, tanto en el área académica como en el área de la industria, sin el manejo adecuado del idioma inglés, tanto la comunicación como la competitividad quedan muy limitados al ámbito local, en los niveles menos competitivos y susceptibles de una rápida obsolescencia. En la academia y la industria, la principal barrera es el idioma y después el financiamiento, incluso el primero limita al segundo. Por ello en este libro se encontrará la siguiente forma de citar los tecnicismos: **frase en español (frase en inglés – acrónimo)**; y con base en ello, se usará el acrónimo como se hace en el argot de las TIC, por ejemplo:

Bus Serie Universal (*Universal Serial Bus* – USB).

Lo que usted obtiene con este libro es 100% aplicable a en la industria en redes, pero dependerá del lector tocar las puertas adecuadas. Personalmente, el desarrollarme profesionalmente en la cambiante, vibrante y retadora área de la electrónica y las telecomunicaciones me ha permitido experimentar los más altos niveles competitivos, en términos de conocimientos, habilidades y de aprendizaje de por vida, en un entorno globalizado que me ha dado la oportunidad de conocer a mucha gente de distintos países, culturas y creencias. Deseo que nuestros lectores y futuros ingenieros puedan experimentar exitosamente su desarrollo profesional, el cual es más fácil de alcanzar en equipo y en comunidad.

José Ignacio Castillo Velázquez – 2023
https://ignaciocastillo.org/

Autor:

José Ignacio Castillo Velázquez cuenta con 27 años de experiencia en TICs, tanto en empresas como en universidades públicas y privadas. Ha participado en 105 proyectos nacionales e internacionales, como líder o miembro en las áreas técnicas y de gestión en 17 países.

Como académico cuenta con 50 publicaciones en revistas y congresos arbitrados; 4 libros y 2 reportes técnicos. Ha impartido 135 cursos de licenciatura y posgrado, así como 171 conferencias magistrales en congresos nacionales e internacionales. Es árbitro en revistas y congresos internacionales tales como *IEEE-LA Transactions*, *Springer-Health and Technology,* IEEE II&TT, ANDESCON, COLCOM, ETCM, LASCCDCN, ICEDEG & ROPEC.

Desde 2008 es profesor investigador de tiempo completo en la carrera de Ingeniería en Electrónica y Telecomunicaciones en la Universidad Autónoma de la Ciudad de México (UACM), donde dirige el *Advanced Networking Laboratory* (ADVNETLAB), así como el seminario y diplomado del mismo nombre. Ha laborado como profesor-investigador de tiempo completo en UPAEP y UTM; y como tiempo parcial en UAM, UDEFA y BUAP. En 2021 fue profesor de posgrado en la Universidad de la Defensa y Fuerza Aérea de México (UDEFA). En 2022 fue profesor visitante en la Universidad Politécnica Salesiana (UPS) en Ecuador.

Como profesional y consultor ha trabajado en *Datacenter Dynamics*, RedUno-Telmex, CEDAT-IFE y DICINET y ha escrito 16 reportes técnicos y 2 artículos en telecomunicaciones y Data Centers; es miembro de International *Computer Room Experts Association* (ICREA) y es miembro de los comités técnicos de redes IEEE LAN/MAN e IEEE *cloud computing*.

Recibió las distinciones internacionales IEEE *Senior Member* (2011) y IEEE *Computer Society Golden Core Member* (2011); mención biográfica en *Who is Who in the world* (2011) y *Distinguished Lecturer* de IEEE *Computer Society* (2015-2017)

Recibió el premio internacional al mejor artículo en *Communications*, al mejor artículo en *Engineering Education* y al mejor artículo en el IEEE ANDESCON 2020. También al mejor artículo en *Engineering Education* en ANDESCON 2022.

En IEEE, de 2007 a 2020 ocupó varios cargos: en IEEE *Computer Society* como miembro del *Board of Governors* y presidente del comité de auditoría; en IEEE *Communications Society* Latinoamérica como secretario y presidente de varios comités; en IEEE MGA Latinoamérica fue secretario, editor en jefe de la revista NoticIEEEro, presidente de varios comités.

El autor obtuvo los grados de Licenciado en Ciencias de la Electrónica, con mención honorífica por la Facultad de Ciencias de la Electrónica, y de Maestro en Ciencias en Dispositivos Electrónicos en el Centro de Investigación en Dispositivos Semiconductores, ambos por la

Benemérita Universidad Autónoma de Puebla en Puebla, México. Los detales los puede consultar en la página web personal https://ignaciocastillo.org/

Agradecimientos

A la Universidad Autónoma de la Ciudad de México (UACM) por otorgarme un año sabático en 2022 para desarrollar esta obra, la cual impactará directamente a la carrera de ingeniería en electrónica y telecomunicaciones.

A mis estudiantes de los cursos del área redes de datos y tesistas del *Advanced Networking Laboratory* (ADVNETLAB), y a los 18 ingenieros e ingenieras egresados.

Al Dr. Gerardo Abel Laguna Sánchez, al Dr. Ricardo Marcelín Jiménez, al Mtro. Pedro Fernando Solares Soto, a la Dra. Rafaela Blanca Silva López, y a la M. en C. Nury Gabriela Ramírez Cely, por su revisión, su arbitraje y sugerencias para mejorar esta obra. Y a la Dra. Carmen Araceli Eudave Loera por la corrección de estilo.

…….

PARTE I: ETHERNET LAN

CAPÍTULO I: LA TECNOLOGÍA DE LEGADO

En este capítulo revisaremos muy brevemente los sistemas precursores de Ethernet, aquellos que en la industria conocemos como *legacy systems*. Los sistemas antecedentes a la conmutación (*switching*) y enrutamiento (*routing*) de la tecnología más generalizada para redes de datos: la Ethernet. Muchas tecnologías compiten, pocas sobreviven, otras sirven de transición, como ISDN y ATM, las cuales tuvieron su apogeo entre 1980 y 2000, mientras que Ethernet, aquella tecnología de conmutación de paquetes, maduraba de 1975 a 1995. Entiéndase enrutamiento o encaminamiento como sinónimos, sin embargo, dado que el término **enrutamiento** esta más extendido en la industria, es el término que usaremos en el libro. Así como en Latinoamérica usamos el término computadora y no ordenador como lo llaman en España.

Antes de iniciar, es conveniente que el lector resuelva la siguiente evaluación diagnóstica. Se hacen 25 preguntas que cubren el mínimo de conocimientos previos en redes de datos, en caso de que ud. no entienda los acrónimos o no pueda responder a las preguntas, entonces le recomiendo estudiar los capítulos 1 al 4 del libro ***Redes de datos: Contexto y evolución,*** disponible en mi página web. https://ignaciocastillo.org/

I.1 EVALUACIÓN DIAGNÓSTICA

1. Explique la diferencia entre las tecnologías conmutación de circuitos y conmutación de paquetes.
2. Indique la función de una red de computadoras.
3. Mencione 5 elementos que conforman una red.
4. Mencione 5 ejemplos de *end system*.
5. Indique la diferencia entre un procesador y un controlador.
6. Indique la diferencia entre RISC y CISC.
7. Indique la función principal de una NIC o WNIC.
8. Mencione 3 ventajas del modelo de referencia ISO/OSI.
9. Bosqueje un mapeo del modelo ISO/OSI al TCP/IP.
10. Describa la función de la capa física del modelo ISO/OSI.
11. Describa la función de la DLL del modelo ISO/OSI (TCP/IP).
12. Indique los elementos que componen una dirección MAC y el número de bits para cada campo.
13. Complete los nombres de los campos para una trama Ethernet II o IEEE 802.3 y el número de bits empleados.
14. Proponga una dirección MAC válida.
15. Describa la función de la capa de Red del modelo ISO/OSI.
16. Indique el rango de direcciones IP públicas para *hosts* en las clases de redes A, B, C, incluyendo sus máscaras de subred.
17. Al crear una red punto a punto entre dos computadoras vía Ethernet, ¿es necesario indicar la dirección IP del Gateway? Justifique su respuesta. Además, explique detalladamente cómo se comprueba la conectividad entre los dos hosts.
18. Describa la función de la capa de transporte-ISO/OSI.
19. Describa la función de la capa de sesión-ISO/OSI.
20. Describa la función de la capa de presentación-ISO/OSI.
21. Mencione un protocolo para cada una de las capas del modelo ISO/OSI.
22. Indique la función del protocolo ARP.
23. Indique la función del protocolo ICMP.
24. Mencione el funcionamiento del proceso ping.
25. Cuando usted asigna una dirección IP y su correspondiente máscara de subred, ¿está configurando una computadora o una NIC (WNIC)? Explique su respuesta.

I.2 Transición de las redes de conmutación a redes de paquetes

Desde los años 70, se buscó que los servicios analógicos de las redes de datos migraran a infraestructura digital, para hacer que todo servicio de voz, datos y video pudiese ofrecerse en una única infraestructura. Sin embargo**,** la idea de la **integración de servicios digitales** se concretó varios años más tarde, para lo cual se fue experimentando con distintas tecnologías. A continuación, se hace una muy breve revisión de dos tecnologías que sirvieron de transición de las redes de conmutación a redes de paquetes y hacia la integración de servicios en Internet: la Red Digital de Servicios Integrados y el Modo de Transferencia Asíncrona **[1]**.

I.2.1 ISDN

Red Digital de Servicios Integrados (*Integrated Services Digital Network* - ISDN) es una tecnología de conmutación y multiplexación que buscó transferir voz, video y datos sobre la red telefónica conmutada (*Public Switching Telephone Network* - PSTN) para ofrecer todos los servicios en una misma red, lo cual permitió la transición de las redes telefónicas analógicas hacia las digitales como una alternativa a los *modems* analógicos **[1]**.

En 1980 la ISDN evolucionó como ISDN de banda angosta (*Narrow*-ISDN) o N-ISDN y para 1988 se ofrecieron los primeros servicios ISDN en USA. La ISDN definió dos interfaces de acceso: la interfaz de tasa básica (*Basic Rate Interface* - BRI) para usuarios finales y pequeños negocios; mientras que la interfaz de tasa primaria (*Primary Rate Interface* - PRI) para empresas u organizaciones. Para tales interfaces se usaron 3 tipos de canales: un canal B de 64 Kbps para voz, otro para datos y un canal D de 16 Kbps para señalización, el cual permite el control de los canales B.

- Un BRI se compone de 3 canales:
  2 canales B y 1 canal D (BRI -> 2B + 1D)
- Un PRI se compone de 24 canales:
  23 canales B y 1 canal D de 64 Kbps (PRI -> 23B + 1D).

¿Qué se hacía cuando se requería un mayor ancho de banda?

Entonces se usaba multiplexación para unir canales B y obtener, por ejemplo, 4B para alcanzar 256Kbps; pero también se podrían usar canales de 64 kbps para sub multiplexar y obtener 2 canales de 32Kbps u 8 canales 8Kbps. Tanto BRI y PRI (ITU-T I431) usaban banda base para

transmitir entre 300 bps y 2 Mbps, constituyendo, los servicios "ISDN de banda base", que no soportaban ni video ni imágenes. La ISDN era cara y no resolvió los problemas que prometía, de modo que tuvieron que buscarse otras tecnologías.

Por ello, en 1985 se formó el grupo que desarrolló la ISDN de banda ancha (*Broadband ISDN*) o B-ISDN de 1.5 Mbps y para 1986 se adoptó el modelo ATM (Asynchronous Transfer Mode) para B-ISDN.

En 1995 se publicaron las "*ISDN yellow pages*", vía la ITU, pero en poco tiempo se convirtió en una tecnología *legacy*, ya que tuvo una rápida obsolescencia, sustituida por ATM y, a su vez, por la tecnología el Protocolo de Internet: IP (*Internet Protocol*).

En 1996 se introdujo voz sobre IP: VoIP (*Voice over IP*) comercial, primero en Finlandia y después en EUA, y paulatinamente en el resto del mundo. Entonces también se usaron otras tecnologías como *Frame Relay* (VoFR) y ATM (VoATM).

En 1999 el tráfico en Internet mundial superó el tráfico en la PSTN/ISDN, vislumbrando así la caída del *legacy system*, cuya eliminación completa era cuestión de tiempo, en función de que el mercado hiciera la sustitución de la infraestructura PSTN que se tendió por todo el mundo desde 1844. En México la ISDN estuvo disponible de manera incipiente en 1990, año en el que se privatizó Telmex, y toda esa década, para el siglo XXI se le consideró *legacy system* **[1]**.

I.2.2 ATM

El modo de transferencia asíncrona *(Asyncronous Transfer Mode* - ATM) es una tecnología de conmutación y multiplexación para transferir voz, video y datos a alta velocidad, a través de redes públicas y privadas, para lo cual se estandarizó vía la Unión Internacional de Telecomunicaciones (*International Telecommunication Union - Telecommunication Standardization Sector* - ITU-T), después de ser desarrollado por Cisco, Sprint, Northern Telecom y NET/ADAPTATIVE en 1991, vía el foro ATM. Esta tecnología combina la conmutación de circuitos con la conmutación de paquetes, el objetivo era ofrecer B-ISDN.

Para realizar enlaces punto a punto ATM, se usaron 2 tipos de interfaces: una es la interfaz de red de usuario (*User Network Interface* - UNI), la cual sirve para conectar los *end systems* con *switches*, y la otra es la interfaz de red a red (*Network-Network Interface - NNI*), la cual sirve para interconectar *switches*. La tabla I.1 muestra los tipos de interfaces, velocidades de transferencia y medios físicos. Los protocolos estandarizados para ATM quedaron con las denominaciones IEEE 802.3 e IEEE 802.5. En enero de 1994, se liberó el RFC 1577 IP sobre ATM (*Classical IP and ARP over ATM*) y en 1998, fue sustituido por el RFC 2225. Algunos ejemplos de *switches* ATM ofrecidos por la marca Cisco son el Catalyst 8540 MSR, el Catalyst 8510 MSR, y el LightStream 1010 **[1]**.

	Tipo de interfaz	**Velocidad de transferencia (Mbps)**	**Medio físico**
DS-0			
DS-1	T1 /(EUA)	1.544 (23 B)	Par trenzado
	E1 / (Europa)	2.048 (30 B)	Par trenzado y coaxial
DS-3	T3	44.736	Cable coaxial
	E3	34.368	Cable coaxial
SONET (*Synchronous Optical Network*) / **SDH** (*Synchronous Digital Hierarchy*)	OC-3	155.52	Fibra óptica mono y multimodo
STM (*Synchronous Transport Module*) Formato de transmisión básico para SDH	STM 1	155.52	UTP - Cat 5
	OC-12	622.08	Fibra óptica monomodo
	OC-48	2,488.32	

Tabla I.1 Tipos de interfaces físicas más comunes.

I.3 Resumen histórico de Ethernet, ISO/OSI y TCP/IP en el siglo XX

En la década de los años 60, nacieron y proliferaron las redes de computadoras de área local (*Local Area Network*-LAN), una vez que se creó y maduró la tecnología de conmutación de paquetes o mensajes, misma que se aplicó en 1969 para tener las primeras redes de área metropolitana (*Metropolitan Area Network* - MAN) operando con la red de la agencia de proyectos de investigación avanzada (*Advanced Research Proyects Agency Network* - ARPANET) en EUA, interconectando así, distintas ciudades dentro de un mismo estado. A finales del mismo año, ARPANET creció para convertirse en una red de área amplia (*Wide Area Network*-WAN), abarcando así distintos estados y eventualmente todo el país **[2]**.

En términos tecnológicos entre 1969 y 1973 se emplearon los *Interfaz Messagge Processor* (IMP), los cuales eran minicomputadoras de tercera generación, que permitieron interconectar *mainframes* para ARPANET, vía el programa de control de red (*Network Control Program-NCP)*, mientras que la comunicación a los nodos distantes se hizo vía la PSTN, empleando *modems* a 56Kbps. En la década de los años 70 se desarrollaron varios protocolos para redes de tipo propietario, de las distintas compañías que producían computadoras y que también competían en la industria de las redes de datos, como *Xerox PARC, Ethernet, Novel Networks Protocol, DEC Protocols, IBM Protocols,* etc.

En 1973 ARPANET sustituyó al NCP por el Protocolo de Control de Transmisión (*Transmission Control Protocol*-TCP) y los IMP fueron sustituidos por computadoras con software más especializado, recibiendo el nombre de *gateways,* liberándose también el Protocolo de Transferencia de Archivos (*File Transfer Protocol* - FTP) y el correo electrónico (*e-mail*).

En 1974 se mencionó, por primera vez, INTERNET, pero en realidad, el concepto se desarrolló más tarde. Para 1975, ARPANET ya era una red completamente operativa. En toda la década de los años 70, Xerox inventó, patentó, implementó y desarrolló Ethernet. Los protocolos de red más importantes de tipo propietario eran NetBios, Novell IPX/SPX, IBM SNA (1982), IBM APPN (1985-1988), AppleTalk, DECnet (DNA 1974/1976/1980/1982+ISO/1987+TCP), Xerox XNS y BanyanVines. Cinco eran los protocolos implementados en las diferentes redes grandes: TCP/IP, NetBIOS, SNA, IPX/SPX y AppleTalk, sin embargo, la gran pregunta era:**[2]**

¿Cómo hacer a todas las redes interoperables?

En 1979, la ISO generó el primer borrador para la Interconexión de Sistemas Abiertos (*Open Systems Interconnection - OSI*), el cual se venía gestando a partir de los avances de Ethernet. Para 1980, DEC, Intel y Xerox (DIX) publicaron la primera versión de “las especificaciones de la Red

de Área Local Ethernet", en las cuales se describió la arquitectura e implementación del funcionamiento de Ethernet, con base en un modelo funcional de 2 capas [3]:

- La Capa Física (*Physical Layer*- PL) o capa de nivel 1 y
- la Capa de Enlace de Datos (*Data Link Layer* - DLL) o capa de nivel 2.

En 1983, Ethernet evolucionó y se publicó como el estándar internacional IEEE 802.3. En 1984, ISO liberó el primer estándar para sistemas abiertos, el ISO 7498:1984, un modelo de referencia OSI que aseguró la compatibilidad e interoperabilidad entre las distintas tecnologías de redes, con base en el trabajo emprendido por Ethernet y TCP/IP [4]. En 1989, se liberó el ISO 7498-2:1989 como la segunda parte del estándar, para tratar el tema de la arquitectura de la seguridad. En 1994, se liberó el estándar ISO/IEC 7498-1:1994, el cual reemplazó a la primera edición de 1984. En 1997, el ISO/IEC 7498-3:1997 agregó observaciones para nombres y direcciones [5-7]. Finalmente, en 1999 se publicó la evolución de IEEE 802.3ab para dar paso al Ethernet Gigabit. Todo el material relacionado con el nacimiento y evolución de Ethernet, ISO/OSI y TCP/IP puede consultarse en la referencia 2. Mientras que la figura I.1 se presenta como un resumen, donde se indica una línea de tiempo [2, 8].

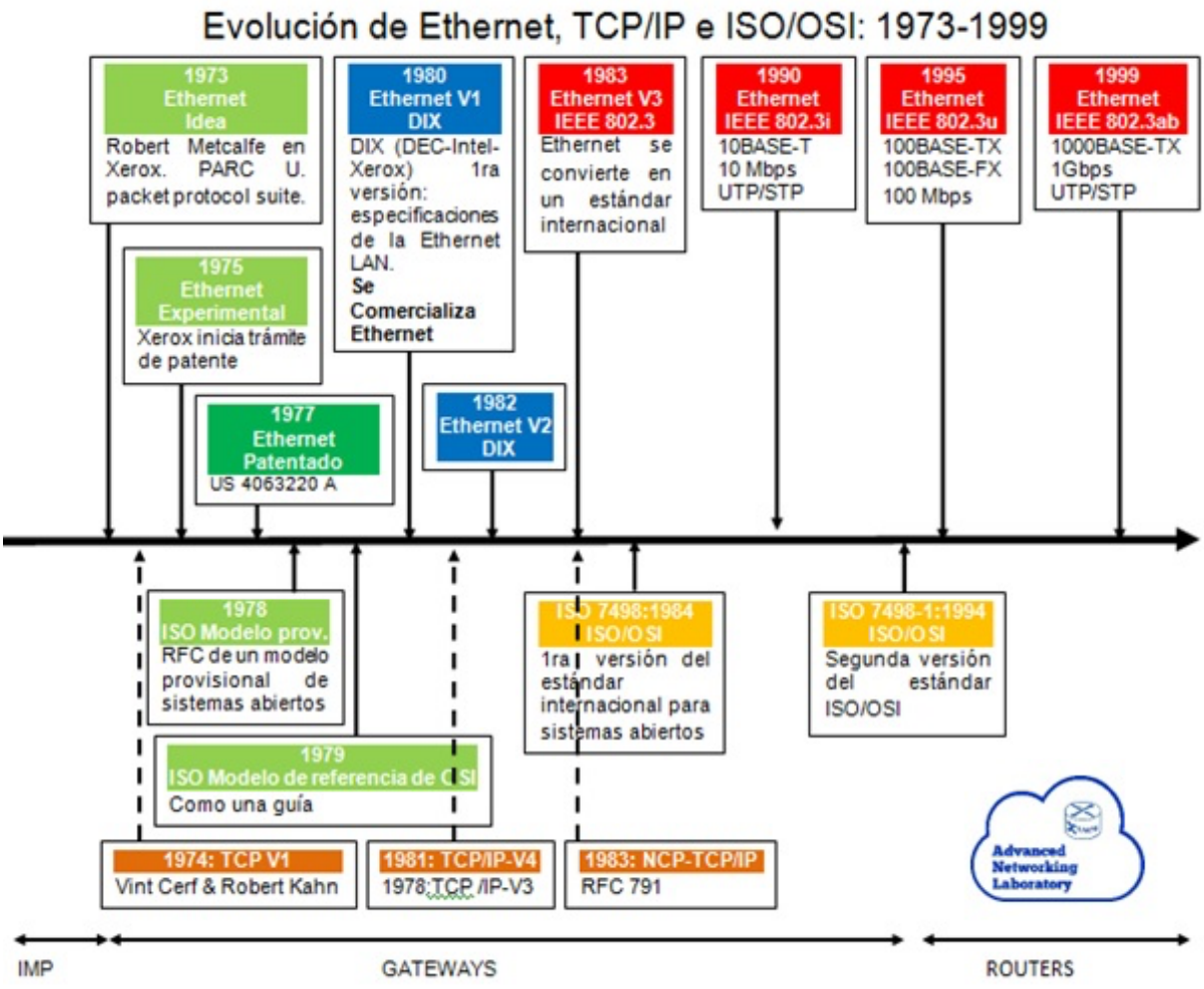


Fig. I.1 Evolución de Ethernet, TCP/IP e ISO/OSI en paralelo con aquella de los IMP, *gateways* y *routers*.

I.4 HUBS

Para extender una red, en un principio se emplearon extensores de red y, como en otros tipos de tecnologías, siempre se empezó usando repetidores. Para las redes de datos se utilizaron los concentradores (*hubs*) como repetidores, los cuales actuaban en la capa 1 del modelo ISO/OSI o TCP/IP.

I.4.1 El nacimiento de los *hubs*

El nacimiento de los *hubs* Ethernet se dio en 1990, con la aparición del estándar IEEE 802.3i (10BASE-T), o Ethernet de 10 Mbps, cuyo tipo de transmisión es banda base y par trenzado (hasta 100 m por segmento) como medio. Posteriormente, aparecieron las tarjetas de red (*Network Interface Card*- NIC) de Ethernet, con conectores RJ 45, para dar paso a la topología de estrella, la cual tomó el lugar de la popular topología de bus de la década de los años 80. Para soportar los 10Mbps de Ethernet, el cable UTP usado en las redes Ethernet (*Token Ring* [IEEE 802.5] y ATM 25) tuvo que ser cable categoría 3 (ANSI/TIA/EIA 568-1991), diseñando para el transporte de datos de hasta 10Mbps; era un cable de clase "c" especificado para enlaces o canales de hasta 16 Mhz. Los *hubs* entonces contaban con entre 4 y 8 puertos de interconexión. En 1990, apareció el primer *switch Ethernet* y, en 1992, el primer *switch fast Ethernet*, sin embargo, el costo era demasiado alto, comparado con los *hubs* y los *bridges*, por lo que su popularidad entre la mayoría de los usuarios tendría que esperar algunos años **[1]**.

El cable UTP categoría 3 se estandarizó en 1991, a 110 años de que Alexander Graham Bell inventara y patentara el UTP en 1881.

En este punto vale la pena mencionar que las redes LAN, utilizadas particularmente en la industria automotriz, empleaban IEEE 802.4 o Token Bus, mismas que usaban el estándar 10BASE-5 (requerían *transceiver* externos a la NIC, con conectores BNC y un máximo de 500 m por segmento) y el estándar 10BASE-2 (los *transceivers* estaban incluidos en la NIC, 185m por segmento, conector BNC).

En 1995 aparecieron las 2 versiones de fibra óptica: 10BASE-FL (2 km por segmento) y el estándar 10BASE-FB (2 km por segmento).

Topología de red: *La topología de una red describe el diseño (layout) del cableado, dispositivos y los caminos empleados para la transmisión de datos. Cada red tiene una topología física (arreglos de host, tarjetas y cables), tales como, BUS, RING (anillo sencillo o doble), STAR (estrella) o una combinación y una topología lógica definida por los caminos que toman las señales a través de la topología física de un punto a otro* ***[1]****.*

I.4.2 El apogeo de los *hubs*

La plenitud de los *hubs* se experimentó en 1995 con la aparición de 2 estándares:

A) El estándar IEEE 802.3u (100 BASE-TX), conocido como *Fast Ethernet* o *Ethernet de 100 Mbps*, entonces aparecieron las *NIC Fast Ethernet* y los fabricantes de equipos de redes actualizaron sus *Ethernet hubs* hacia los *Fast Ethernet Hubs*. A estos *hubs* se les consideró de "segunda generación", porque presentaban mejores características, como algunas funcionalidades que permitían monitorear el tráfico vía SNMP (*Simple Network Management Protocol*) y RMON (*Remote Monitor*), las cuales están presentes, por ejemplo, en los equipos Cisco 1538 series Micro Hub 10/100, de 8 puertos **[9]**.

B) El estándar ANSI/EIA/TIA 568A-1995, definió a los cables de las categorías 4 y 5. El cable categoría 4 fue diseñado para el transporte de datos hasta 16 Mbps, un cable para enlaces o canales de hasta 20Mhz; el cual fue usado por un periodo muy breve y principalmente para redes LAN Token Ring (IEEE 802.5) de IBM; mientras que el cable categoría 5 fue diseñado para un máximo de 100 Mbps, especificado para enlaces o canales de hasta 100Mhz **[1]**.

En 1995 (como en la actualidad), el Ethernet IEEE 802.3 ya era el estándar para LAN más empleado en el mundo.

En 1996, el fabricante 3COM produjo su *hub Ethernet* (10Mbps) *SuperStack* II *Hub* 10 de 24 puertos. Por su parte, Cisco ofrecía sus *hubs* "Cisco Fasthub Series 100, 200 y 300", o repetidores *Fast Ethernet (FE)*, todos con interfaces 10BASET y 100BASETX, con 4, 8, 12 y16 puertos *Fast Ethernet*.

En 1998 Cisco anunció que sus tres series de *hubs* dejarían de producirse y de venderse en 1999, para ser sustituidos por la última generación de *hubs*: la serie 400. Los *hubs* Cisco de la serie "*Cisco Fast Hubs 400 Series Repeaters*" contaban con interfaces 10BASET, 100BASETX, 100BASEFX,

de 12 y 24 puertos FE, en la época en la que el cable UTP categoría 5 era el popular [10]. El símbolo del *hub* se indica en la figura I.2.

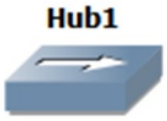


Fig. I.2 Símbolo estándar del *hub*.

Para 1996 se tenían ya en EUA, las primeras implementaciones del estándar IEEE 802.11 (WiFi) en la banda industrial, científica y médica (*Industrial-Scientific-Medical* - ISM) de 2.4Mhz, con velocidades de transmisión en el orden de 64 y 128 Kbps. Mientras que el estándar IEEE 802.3 (Ethernet) empleaba *Carrier Sense Multiple Access/Collition Detection* (CSMA/CD), el estándar IEEE 802.11 (WiFi) usaba ya *Carrier Sense Multiple Access/Collition Avoidance* (CSMA/CA). En esa misma época, los conjuntos de protocolos de red más importantes provenían del protocolo ISO/OSI y del protocolo TCP/IP (originalmente usando en la WAN ARPANET-1969/Internet-90 y redes grandes, desarrolladas en UNIX). La figura I.3 muestra la simbología para interconectar *hubs* y *hubs* con *host*.

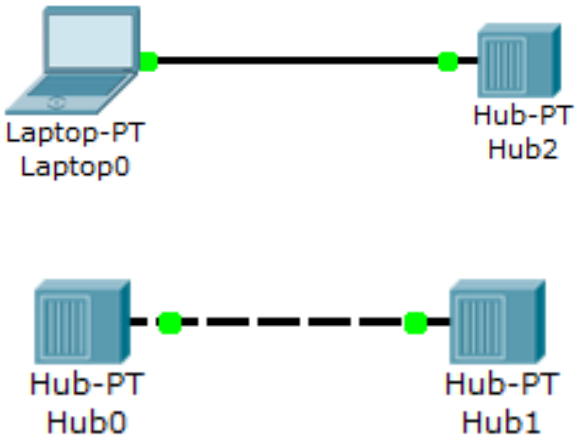


Fig. I.3 Cableado para la interconexión *hub- host (directo) y hub-hub (cruzado) [Símbolos de Cisco Systems]*.

I.4.3 La caída de los *hubs*

En 1997 apareció el primer *switch* Giga Ethernet, lo cual permitió que los switches Ethernet y *fast* Ethernet redujeran mucho de precio y, eventualmente, fueran la base para desplazar a los *hubs*.

En 1999 apareció el estándar IEEE 802.3ab (1000BASE-T), el Ethernet de 1000 Mbps o 1Gbps, lo que marcó también el inicio de la obsolescencia de los *hubs, así como* el impulso definitivo para que los *bridges* y *switches* quedaran como los extensores de redes. Con la finalidad de dar vida a los *hubs* que las compañías tenían almacenados todavía y, como parte de un proceso de transición tecnológica, se recomendó el uso de los *hubs*, como complemento de los *switches*, donde no se requiriera un ancho de banda dedicado; esto quedó como una tendencia general desde 1999. Cisco dejó de producir la serie *Fast Hub* 400 (de 12 o 24 puertos) en 2001 y ya no la vendió en 2002, recomendando a sus usuarios reemplazar los *hubs* por los *switches* Cisco *Catalyst*, serie 2950; a la vez que resaltó las ventajas de estos *switches* para redes pequeñas y medianas, indicando que, además de datos, ya soportaban audio y video **[1]**.

El *Fast Hub* 400 tenía capacidades para monitoreo y análisis vía el Protocolo de Gestión de Red Simple (*Simple Network Management Protocol* - SNMP) y soportaba la Base de Información (*Management Information Base* - MIB) II, Ethernet MIB y Mini-RMON MIB para alarmas y eventos; además este modelo ya era configurable. Hoy en día, aunque los hubs son obsoletos, un *hub* Ethernet de 8 puertos de 10/100 Mbps marca 3COM, por ejemplo, en Amazon; un hub "nuevo" se puede comprar por 60 dólares o usado por 7 dólares.[1]

También cabe aclarar que los primeros *switches* de capa 2 de Cisco, los *EtherSwitch*, iniciaron su obsolescencia en 1996, por lo que en 1999, ya se sugerían como complemento de los switches. La figura I.4 muestra un resumen, con forma de caligrama, de la historia de la tecnología *hub* Ethernet.

Entre 1992 y 1993, mientras yo estudiaba la Licenciatura en Electrónica, también trabajé en la empresa DICINET en la ciudad de Puebla, en México, allí se instalaba, configuraba y hacía *troubleshooting* a algunas redes corporativas. En esa época la topología más popular era la de tipo BUS y se empleaba el estándar 10BASE-2 con tarjetas y sistemas operativos de red de *Novel*

[1] Véase: http://www.amazon.com/3Com-3C16700A-OfficeConnect-8-Port-Ethernet/dp/B0000304ZO.

Netware. En ese tiempo, el trabajo de administración de redes se realizaba empleando sólo CLI como interfaz para la configuración, monitoreo, actualización y resolución de problemas [1].

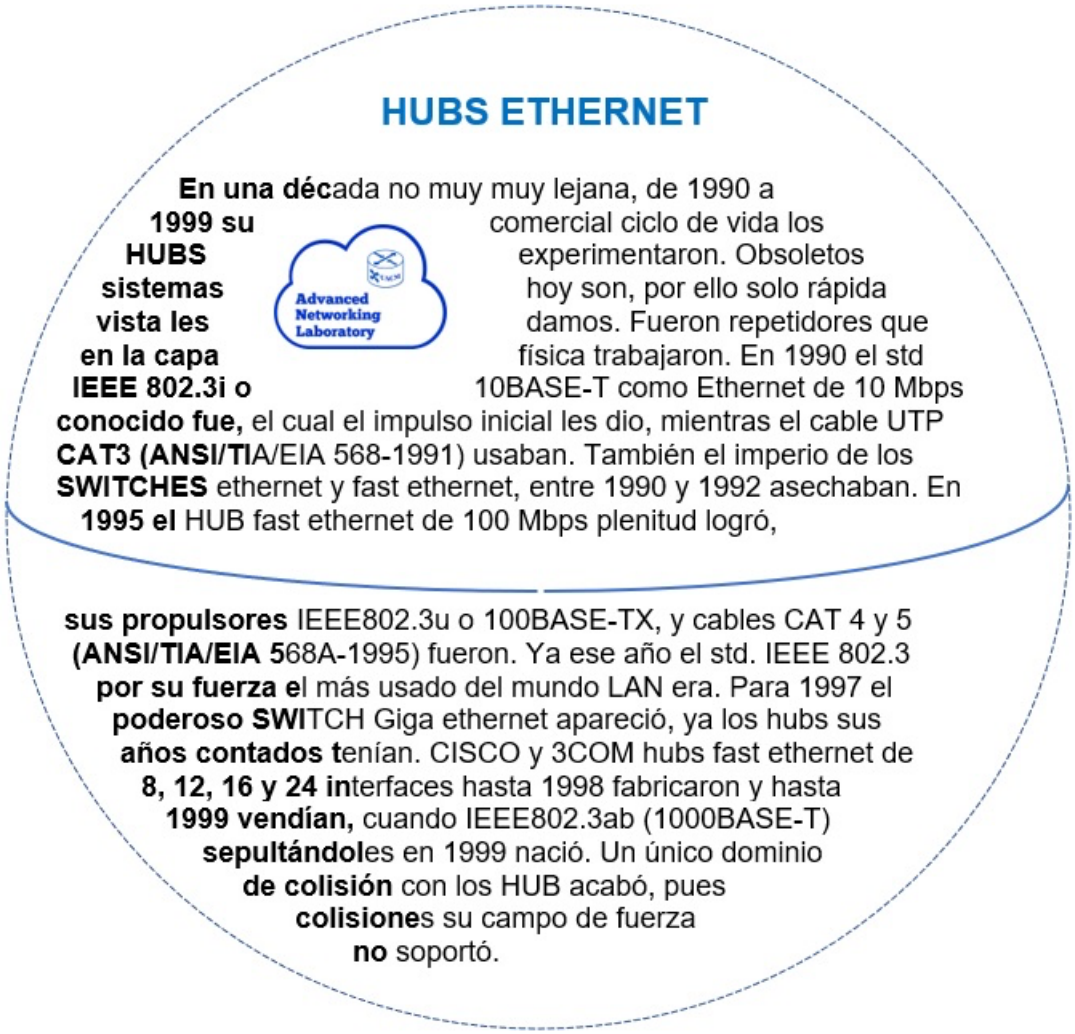


Fig. I.4 Resumen de la historia de la tecnología HUB Ethernet en un caligrama.

I.5 Circuitos Ethernet LAN con base en *hubs*

A manera de ejemplos, se presenta una red LAN creada con base en un *hub* y 4 *end systems o hosts*, como se indica en la figura I.5. Después de asignar las direcciones IP y máscaras de subred, se comprueba la conectividad mediante el comando *ping,* verificando el funcionamiento correcto de los protocolos ARP e ICMP, tanto para cuando se envían paquetes de manera individual como para cuando se envían paquetes simultáneos de manera masiva entre los *hosts*. Para esto se usa el simulador Cisco *Packet Tracer*, eligiendo el modo simulación y editando el filtro de modo que sólo aparezcan los protocolos ARP e ICMP, ya que son los empleados en el proceso *ping*. Una vez terminado el circuito, probamos la conectividad enviando paquetes PDU, desde un *host* a otro, o directamente probamos la conectividad con la orden *ping*. Con ello se puede observar el flujo de los paquetes ICMP y ARP desde el origen hacia el *hub* ***[1]***.

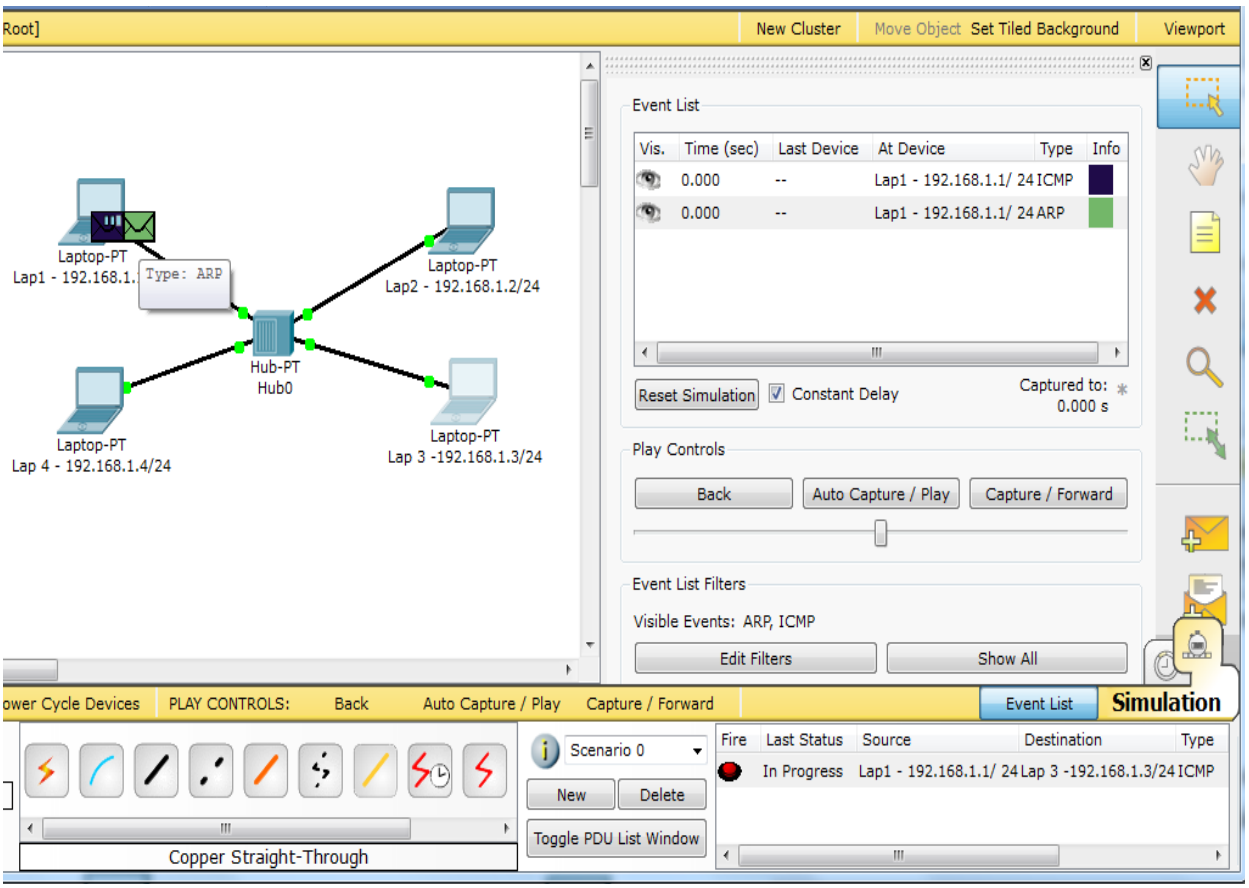


Fig. I.5 Red LAN con *hub* y el envío de paquetes (PDU) entre *hosts*.

Una vez que el paquete ARP llega al *hub,* encapsulado en la trama, el *hub* – siendo un repetidor–, inunda (*flooding*) a la red reenviado la trama (L2) hacia todos los miembros de la misma, excepto por la interfaz origen, como se muestra en la figura I.6, en la cual aparecen también los detalles de la trama y el protocolo ARP entre las capas L1 y L2 del modelo TCP/IP.

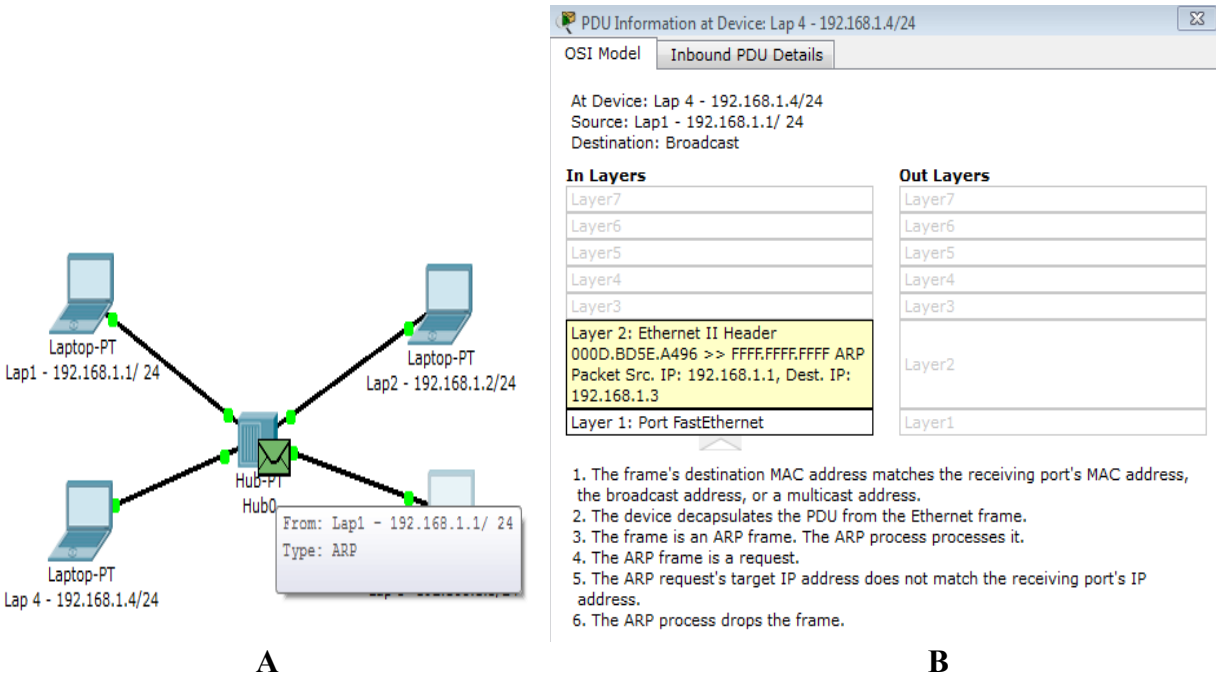


Fig. I.6 A) La trama que contiene al paquete ARP llega al *hub*. B) Detalles de recepción de la trama en L1 y L2.

Con la finalidad de ser más explícito, se coloca la figura I.7 en formato grande, para visualizar mejor el proceso de inundación.

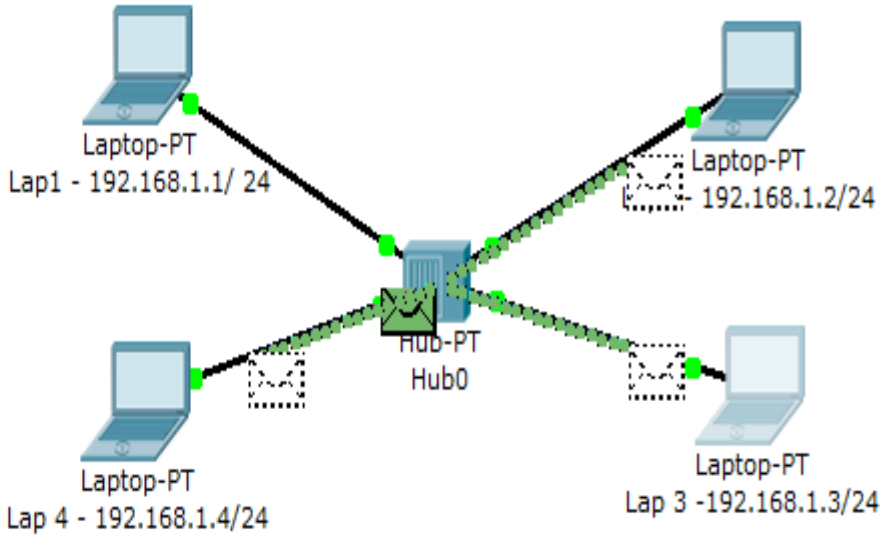
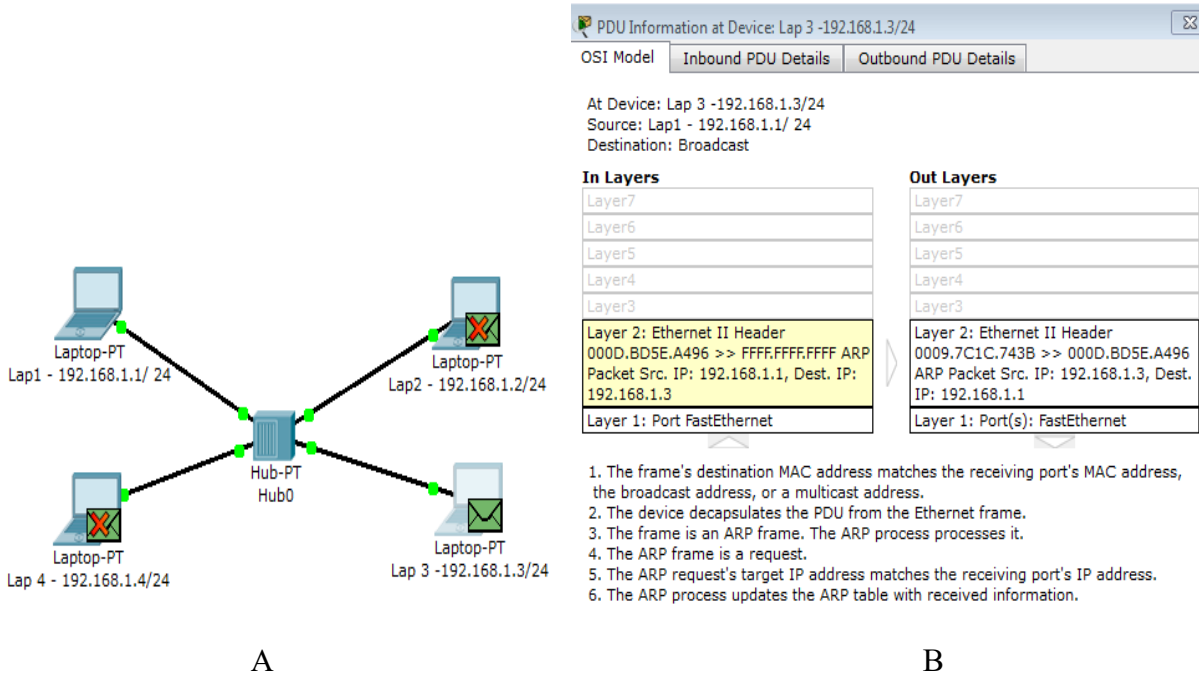


Fig. I.7 El *hub* inunda la red reenviando la trama convertida en bits a través de todas sus interfaces.

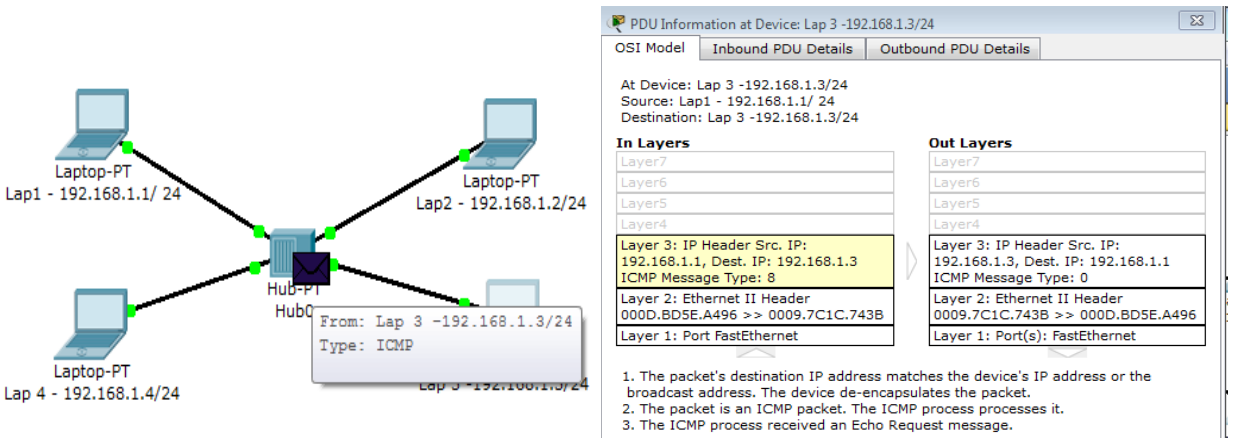
En la figura I.8 muestra la llegada de la trama a cada *host* y cómo es que aquellas NIC que no identifican a la trama la desechan, mientras que el *host* objetivo recibe los bits por el medio, así como la trama desencapsulada, atiende el requerimiento y envía de regreso el paquete ARP, a través de la trama de regreso al *hub*.



A B

Fig. I.8 A) El *frame* ARP-*request* llega al *host* destino. B) El proceso ARP- *request* llegó al destino y se actualiza la tabla ARP del *host* destino, por lo que se completa la mitad del proceso ARP en capa 2.

Una vez que el paquete ARP llega al *host* original, se actualiza la tabla ARP del *host* origen, terminando así el proceso ARP. Entonces es el turno del proceso ICMP, el cual forma al paquete ICMP, mismo que estaba a la espera en modo *buffer*, y queda listo para enviarse al *hub.* Los detalles se muestran en la figura I.9. La figura I. 9A muestra que el *frame* ICMP-request, desde LAP 1, llega al *hub* y éste inunda la red, entonces llega al *host* destino y se actualiza su tabla, mientras que en los otros *hosts*, tal *frame* se desecha, y se completa la mitad del proceso ICMP (L3). En la figura I.9B se muestran todos los detalles de lo que ocurre en cada capa.



A) B)

Fig. I.9 A) Frame ICMP-*request* desde LAP 1 al *hub*. B) Muestra los detalles de cada capa.

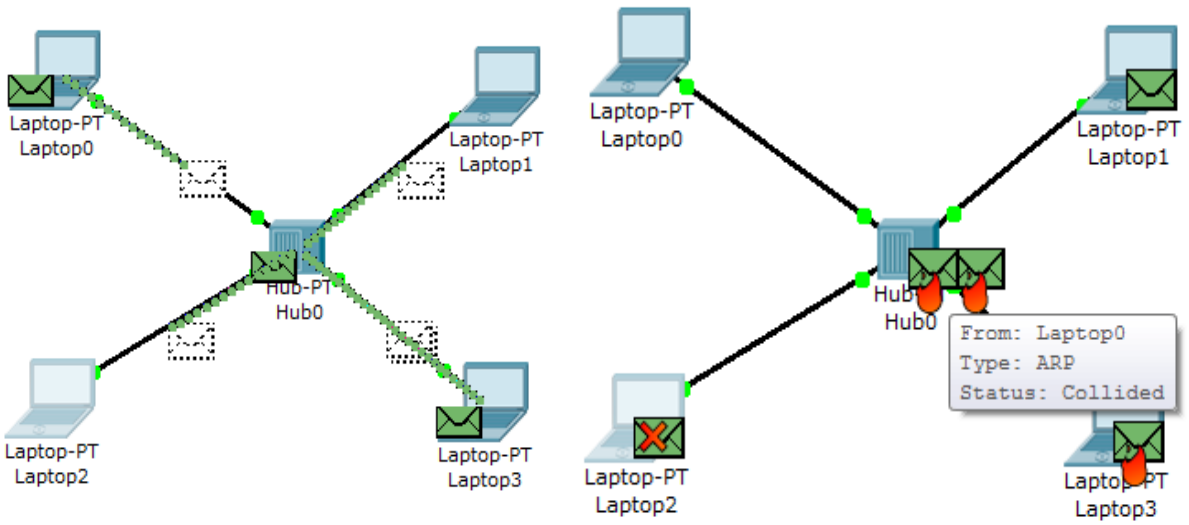
El proceso ICMP termina cuando LAP 3 responde y la trama ICMP-*response* llega al *hub*, éste inunda la red y la trama llega a la LAP 1, respondiendo al proceso de PING. De esta manera, queda ejemplificado el funcionamiento de un *hub*.

Sin embargo, ¿qué sucede cuando en esta LAN con un *hub* se envían varios paquetes de manera simultánea, desde un *host* a otro o al resto de los *hosts*?

I.6 Dominio de colisión

La figura 1.10 muestra cómo se generan varios paquetes y cómo se produce una colisión de tramas, esto sucede porque el *hub,* al ser un mero repetidor cuyo funcionamiento se da exclusivamente en la capa física (o capa 1), tiene un único **dominio de colisión,** es decir, todas sus interfaces pertenecen a un único dominio de *broadcast*.

Y este es el grave problema que presentan los hubs: *las colisiones, ya que todos sus puertos se encuentran en el mismo dominio de colisión. La solución, está en los* bridges, los cuales operan en la capa de enlace de datos *(o capa 2), los cuales aprenden, reenvían y eliminan bucles usando el protocolo de podado de árbol (Spanning Tree Protocol - STP), pero existen problemas de* broadcast*, con lo que hay mucho tráfico en la red, una cuestión que resuelven los* switches **[1].**



A) B)

Fig. I.10 A) El *hub* replica los paquetes en el resto de las interfaces. B) Pero, simultáneamente las tramas que salen de los otros *hosts* colisionan con las tramas que vienen hacia cada *host* desde el *hub*.

Es necesario que el lector se asegure de haber entendido cabalmente cada uno de los pasos, ya que este proceso se sigue en toda red cada vez que se envía un ping y, de manera similar, cada vez que se envía cualesquier paquete, mensaje o archivo desde una computadora a otra. En este punto el lector debe tener claras las diferencias entre procesos ARP y paquetes ARP, así como entre los procesos ICMP y paquetes ICMP. Si tiene dudas, consulte la referencia **[2]**.

I.7 PRÁCTICA 1: LAN con base en *hub*

El objetivo de esta práctica es que el lector simule una LAN con base en un *hub*, envíe paquetes entre los *hosts* y observe las colisiones que se generan, procurando reproducir cada uno de los pasos seguidos en la explicación dada en este capítulo.

Actividad 1: Acceda al simulador para crear un circuito con un *hub* y 4 computadoras, asigne las correspondientes direcciones IP, con la máscara de subred natural, como se indica en la figura I.5.
Actividad 2: Envíe un ***ping*** entre una computadora y otra para observar el flujo de bits y tramas que contienen los paquetes ARP e ICMP, desde el origen hacia su destino en la LAN.
Actividad 3: Envíe paquetes desde un equipo hacia el resto de los equipos y ejecute, de manera simultánea, para percatarse de que se presenten colisiones.

CAPÍTULO II: CONMUTACIÓN EN LAN

Los *bridges* (puentes) se consideran *switches* de capa 2, se inventaron en 1983 para extender redes, pero, al igual que los *hubs* de capa 1, generaban tormentas *broadcast*; la solución fue el *switch* de capa 3, cuyo uso masivo inició en 1999. Los switches más modernos son llamados switches de capa 4, ya que cuentan con una capa adicional de software que los habilita para generar y gestionar políticas de tráfico, priorizar a cierto tipo de paquetes o incluso aplicar algunos principios de "corta fuegos" (*firewall*).

II.1 *Ethernet switching*: L3

En 1983, *Digital Equipment Corporation* (DEC) inventó el *bridge*, el cual interconectaba redes de *mainframes* y actuaba en la capa 2 del modelo ISO/OSI, sin embargo, generaban tormentas de difusión (*broadcast)*, pero este inconveniente se resolvió con el conmutador (*switch)* de capa 3. Cuando se habla de *switches*, se debe especificar la tecnología. Los *switches* para la red telefónica son muy antiguos, pero si nos referimos a redes de datos podemos encontrar *switches* para tecnologías como ATM, la cual podría trabajar con redes de conmutación de circuitos como PSTN, así como con las redes de conmutación de paquetes: ISDN, *Token Ring; FDDI; Fibre Chanel; InfiniBand o Ethernet*, entre otros. La figura II.1 muestra los diagramas correspondientes a *switches* usados en tecnologías *legacy*: *Frame Relay* y ATM [1].

Fig. II.1 Diagramas correspondientes a switches FR, ATM.

Un *switch* es un equipo conmutador electrónico para redes de datos, el cual provee un enlace entre sistemas de trabajo (impresoras, computadoras, teléfonos), una conmutación inteligente de los datos dentro de una red local y trabaja en la capa 3 del modelo ISO/OSI o TCP/IP. En la figura II.2 se muestra a un *switch* comunicando a 4 computadoras para crear una LAN. Nótese el símbolo de un *switch* Ethernet consiste en dos flechas a la izquierda y dos a la derecha.

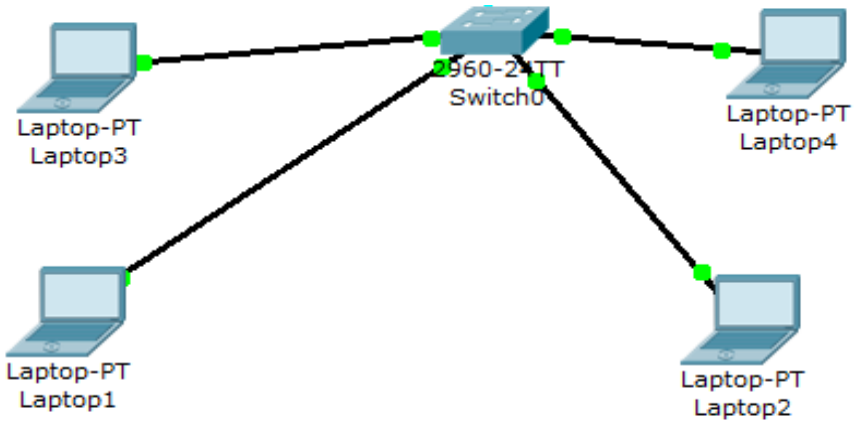


Fig. II.2 Diagrama de un switch de acceso, el cual permite la creación de una LAN.

En 1987 las redes LAN Ethernet, 10BASE T, estaban proliferando en las economías mundiales más importantes, entonces *Vinod Bhardwaj* inventó el primer "switch Ethernet" en San José, California, y, como siempre sucede, tuvo problemas para que una empresa grande invirtiera; por lo que terminó creando su propia empresa, KALPANA Inc. ("*Imaginación*", en idioma hindi).

La tabla II.1 muestra los éxitos de las primeras empresas que representan hitos en el desarrollo de la tecnología de *switches*.

Empresas	Switches comerciales pioneros
1990 KALPANA (En 1994 CISCO *Systems compró* a KALPANA)	*Switch Ethernet LAN* de 7 puertos AUI a 10Mbps. EPS 700, por $11,500 USD.
FORE	*Switch ATM* / ASX100
Grand Juntion	*Switch Fast Ethernet*.
1993 Berkeley Networks	Switch Gigabit para la tecnología FDDI (backbone).
Centillion Networks	*Switch Token-Ring*
1997 Foundry Networks	*Switch Gigabit Ethernet*.

Tabla II.1 Primeros *switches* comerciales.

Los primeros *switches* de 1990 son considerados *switches* de capa 3, estos se inventaron para desplazar a los *hubs* y *bridges*, a los que también de manera popular la gente les llamaba *switches*, porque de alguna manera todos hacían conmutación **[1]**.

El *switch* de la figura II.3 muestran dos *switches* de acceso de capa 2 no configurable, los cuales se pueden encontrar en los *racks* ubicados en las instalaciones de distribución intermedia (*Intermediate Distribution Facilities* - IDF).

En la actualidad, para poder cubrir las necesidades de las redes 2.5 Giga Ethernet (GE), compañías como QNAP, se dedican al almacenamiento con equipos de red (Network-Attached Storage -NAS), también ofrecen algunas soluciones como la indicada en la figura II.6. Estos equipos son adecuados para la llegada del IEEE 802.11ax (Wifi 6-2019) [1024-QAM], el cual ya usa MIMO y MU-MIMO.

Específicamente, el Wi-Fi 6 corresponde al estándar *IEEE P802.11ax-IEEE Draft Standard for Information Technology-Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks -- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment Enhancements for High Efficiency WLAN.*

(A) (B)

Fig. II.3 (A) *Switch* de acceso y (B) *Switch* QNAP QSW-1105-ST para 2.5 GbE, ambos no configurables.

Si nos preguntamos cuántos tipos de *switches* hay, en función de si se les considera de la capa de acceso, distribución o núcleo (*core*), la figura II.4 muestra la respuesta para la gama de *switches* de CISCO, cuyas interfaces son *Fast* Ethernet (FE) y algunas Giga Ethernet (GE). Mientras que la figura II.5 muestra la foto de un *switch* de *backbone*, ubicado en una instalación de distribución principal (*Main Distribution Facility* - MDF). Los *switches* indicados en un recuadro verde hacen referencia a *switches* que son obsoletos, pero funcionales incluso actualmente [1].

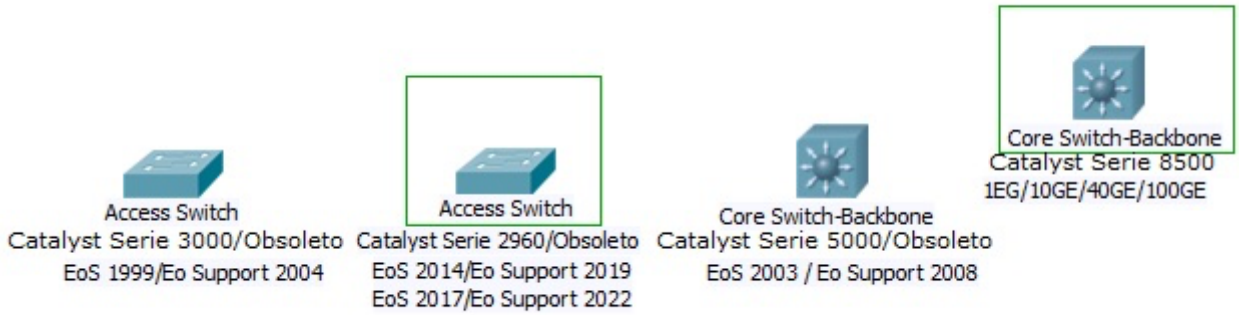


Fig. II.4 Switches Cisco serie Catalyst, en su gama de acceso y núcleo (*Core*).

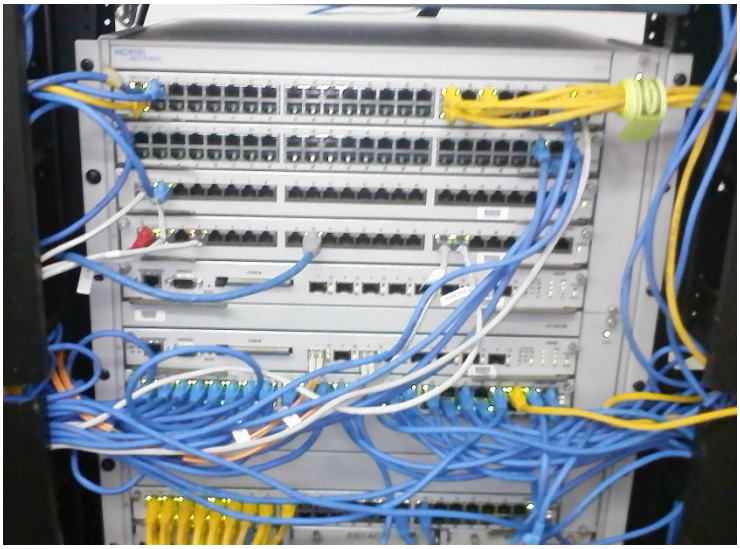
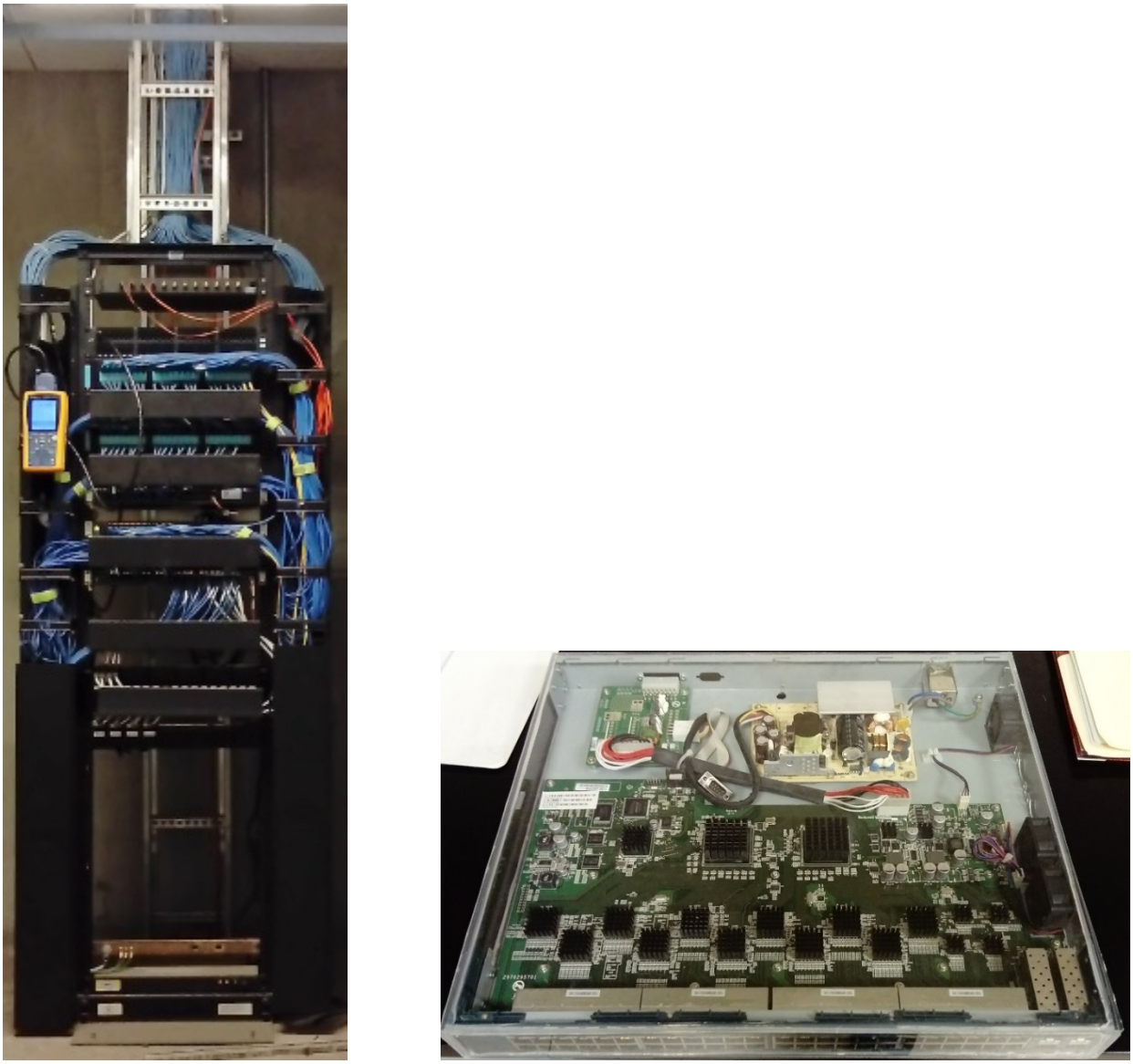


Fig. II.5 *Core switch*, Ethernet Routing Switching, Marca Nortel Networks, ubicado en un MDF.

Además, en la figura II.6 muestro la foto, tanto de un *rack* ubicado en un IDF como de un *switch* de acceso Cisco ESW-540-48 / 4 SPF. A este *switch* le quité la cubierta, para que el lector pueda ver la circuitería interna y fuente de alimentación.



A B

Fig. II.6 A) *Rack* en IDF-2021. B) *Switch* de acceso Cisco ESW540-48 /4 SPF (2009-2019) para montaje en IDF (ADVNETLAB).

II.2 Arranque de un *switch*

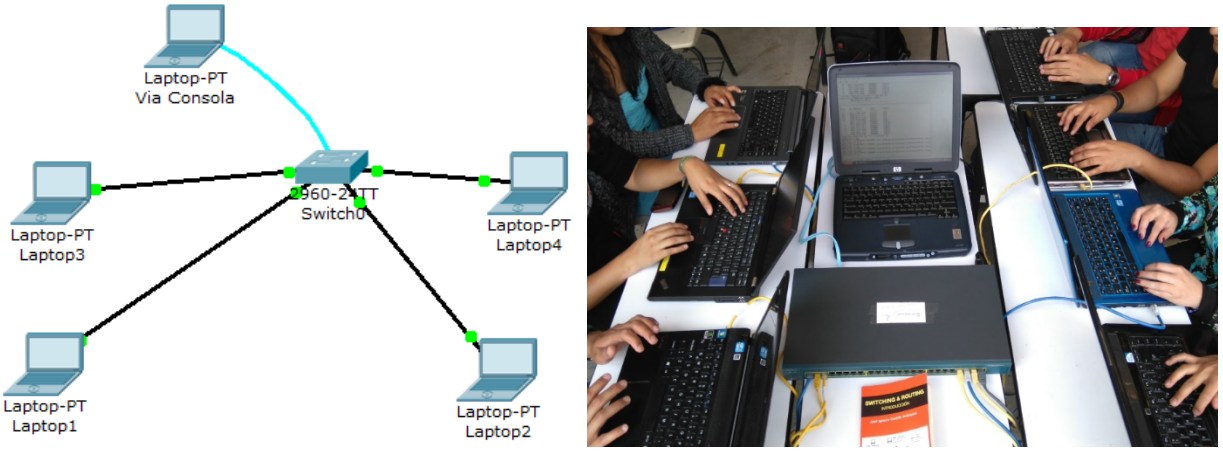
Un *switch,* siendo una computadora de propósito específico –en este caso para telecomunicaciones, en particular para redes de datos–, tiene un arranque similar al de una computadora genérica. Una vez que se arranca un *switch,* después de ejecutarse el programa de arranque y las pruebas POST, el *Internetworking Operative System* (IOS) toma el control del sistema, como se indica en la figura II.7

```
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r) FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0003.E45B.D1B7
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
########################################### [OK]
          Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software – Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013. Cisco Systems, Inc./170 West Tasman Drive/San Jose, California 95134-1706
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25) FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Image text-base: 0x80008098, data-base: 0x814129C4
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0003.E45B.D1B7
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01
Switch   Ports  Model              SW Version            SW Image
*    1   26     WS-C2960-24TT      12.2                  C2960-LANBASE-M
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
Press RETURN to get started!
```

Fig. II.7 El CLI mostrando el arranque de un *switch*

II.3 Circuito LAN con base en un *switch*: Monitoreo y configuración básicas

Ahora para crear una red LAN con base en un *switch*, se realizan las conexiones entre un *switch* de acceso y hosts, como se indica en la figura II.8a, lo cual en la práctica podría verse como en la figura II.8b.

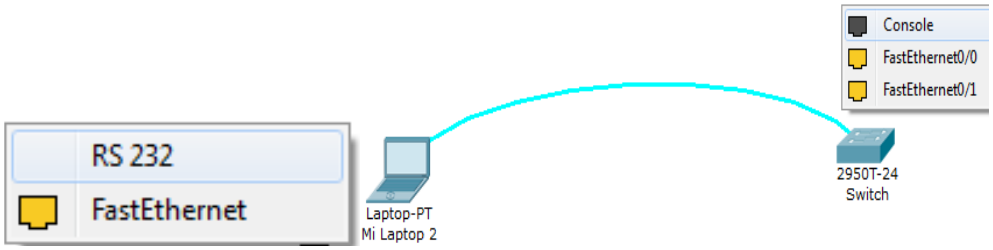


A B

Fig. II.8 A) Conexión a la consola de un switch. B) LAN con switch Cisco C2960-24 con 7 usuarios

Ahora vamos a los detalles. En el simulador se escoge el cable curvo (azul o cable para consola) para conectar la laptop que prestará su pantalla y teclado al *switch* para realizar las actividades de administración de una LAN, esto se realiza mediante las interfaces seriales RS232, como se indica en la figura II.9.

A



B

Fig. II.9. A) Observe el cable de consola. B) Conexión desde PC (RS-232) a SW (Consola).

La comunicación entre la computadora que se conecta a la consola del SW se da vía puerto serial, para ello se debe ejecutar el "programa de software de emulación de terminal", el cual permite comunicar a la PC con un *switch* o *router* u otra computadora. Observe el procedimiento de ejecución y selección de puerto en la figura II.10. La configuración del puerto de comunicación serial se hace en COM 1, COM 2 o COM 3 bajo los parámetros: 9600 baud, 8 data bits, "*No parity generated or checked*", 1 "*stop bit*", "*No Flow Control*".

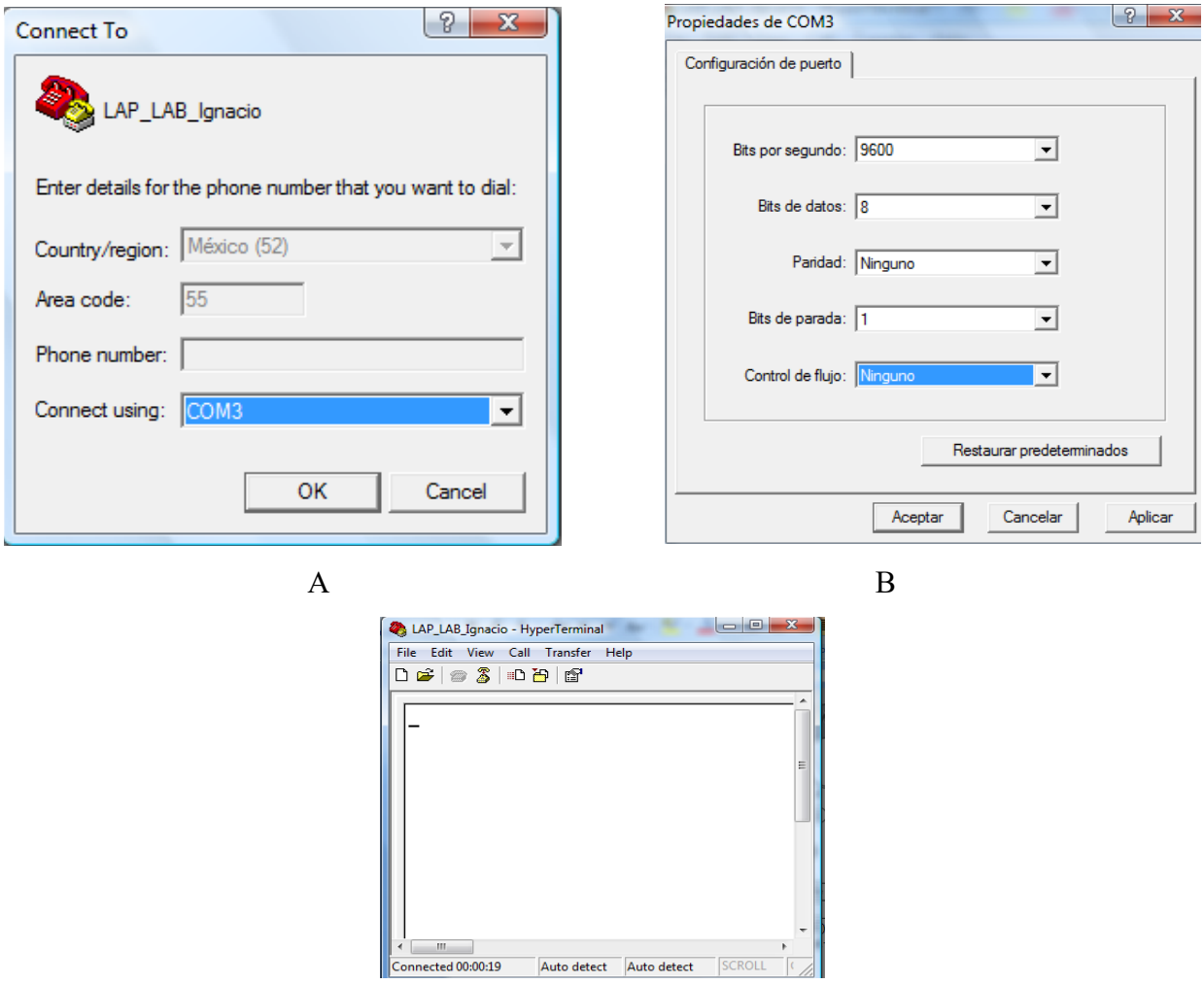


Fig. II.10 A) Ejecución de *Hyper Terminal Private Edition y selección de puerto.* B) Configuración del puerto COM 3 y C) Su respuesta que indica que existe comunicación entre la PC y el *Switch*.

Una vez que nos encontramos en comunicación con un *switch*, la figura II.11 muestra los modos de ejecución, monitoreo y configuración más básicos para un *switch* de Cisco [1].

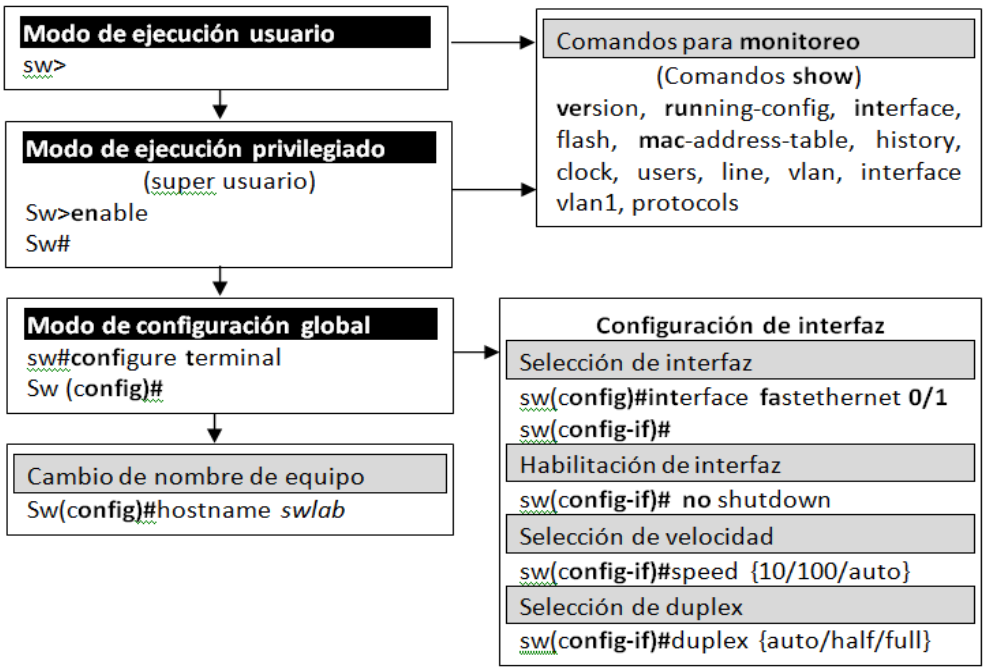


Fig. II.11. Modos de ejecución, configuración y monitoreo de un *switch* CISCO.

Para monitorear a un *switch* y una red, se recomienda ingresar en modo "super usuario". La figura II.12 muestra el resultado de solicitarle su versión del IOS.

```
Switch#show ver
Cisco IOS Software, C2960 Software(C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
System returned to ROM by power-on
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0003.E45B.D1B7
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Hardware Board Revision Number  : 0x01
Switch   Ports  Model           SW Version           SW Image
*    1   26     WS-C2960-24TT   12.2                 C2960-LANBASE-M
Configuration register is 0xF
```

Fig. II.12. Resultado de solicitar la versión del IOS.

La figura II.13 muestra el resultado de solicitarle al switch que presente el contenido de la tabla

MAC correspondiente, indicando los encabezados.

```
Switch#show mac-address-table
        Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.633c.c7e5    DYNAMIC     Fa0/1
   1    0006.2ac8.9db6    DYNAMIC     Fa0/4
   1    0060.3e3b.784d    DYNAMIC     Fa0/2
   1    00d0.ff54.3412    DYNAMIC     Fa0/3
```

Fig. II.13. Resultado de solicitar la tabla MAC.

La figura II.14 muestra los procesos que se ejecutan en el *switch.*

```
Switch#show pro
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID QTy       PC Runtime (ms)    Invoked  uSecs     Stacks TTY Process
   1 Csp 602F3AF0           0       1627       0 2600/3000   0 Load Meter
   2 Lwe 60C5BE00           4        136      29 5572/6000   0 CEF Scanner
   3 Lst 602D90F8        1676        837    2002 5740/6000   0 Check heaps
   4 Cwe 602D08F8           0          1       0 5568/6000   0 Chunk Manager
   5 Cwe 602DF0E8           0          1       0 5592/6000   0 Pool Manager
   6 Mst 60251E38           0          2       0 5560/6000   0 Timers
   7 Mwe 600D4940           0          2       0 5568/6000   0 Serial Backgrou
   8 Mwe 6034B718           0          1       0 2584/3000   0 OIR Handler
   9 Mwe 603FA3C8           0          1       0 5612/6000   0 IPC Zone Manage
  10 Mwe 603FA1A0           0       8124       0 5488/6000   0 IPC Periodic Ti
  11 Mwe 603FA220           0          9       0 4884/6000   0 IPC Seat Manage
  12 Lwe 60406818         124       2003      61 5300/6000   0 ARP Input
  13 Mwe 60581638           0          1       0 5760/6000   0 HC Counter Time
  14 Mwe 605E3D00           0          2       0 5564/6000   0 DDR Timers
  15 Msp 80164A38           0      79543       0 5608/6000   0 GraphIt
  16 Mwe 802DB0FC           0          2     011576/12000  0 Dialer event
  17 Cwe 801E74BC           0          1       0 5808/6000   0 Critical Bkgnd
  18 Mwe 80194D20           4       9549     010428/12000  0 Net Background
  19 Lwe 8011E9CC           0         20     011096/12000  0 Logger
  20 Mwe 80140160           8      79539       0 5108/6000   0 TTY Background
  21 Msp 80194114           0      95409       0 8680/9000   0 Per-Second Job
  22 Mwe 8047E960           0          2       0 5544/6000   0 dot1x
```

Fig. II.14. Resultado de solicitar los procesos que se encuentran ejecutándose en el *switch*.

La figura II.15 muestra el contenido de la memoria *flash*.

```
sw#show flash
Directory of flash:/
2 –rwx 2667024 0:03 i6q4ysk36.bin
3 –rwx 2667024 0:03 i6q4ysk36.txt
4 –drwx 2667024 0:03 sistema
```

Fig. II.15. Resultado de solicitar el contenido de la memoria *flash*.

Una vez que un aprendiz de administrador de red domina el monitoreo, su siguiente tarea es realizar configuraciones básicas, tales como cambiar el nombre del *switch*, ingresar a las interfaces para habilitarlas o deshabilitarlas y guardar la configuración que se ha cambiado para que cuando se borre la RAM no se pierda y se escriba en la memoria *flash*. La figura II.16 muestra cómo realizar el guardado de configuración desde la memoria RAM hacia la memoria *flash*. En la figura II.11 se mostró cómo cambiar el nombre de un *switch* vía la orden *hostname*, y también se mostró el detalle de cómo habilitar una interfaz del *switch*.

```
sw#write
o
sw#wr
```

Fig. II.16. Resultado de solicitar el contenido de la memoria *flash*.

En caso de ser necesario, use la orden "*copy flash*: config.old config.txt", para respaldar archivos en la memoria *flash*.

II.4 PRÁCTICA 2: LAN con base en switch

El objetivo de esta práctica es que el lector simule una LAN con base en *switch,* con la topología indicada en la figura II.8. Envíe paquetes entre los *hosts* y observe el comportamiento de la red, realice las siguientes actividades tanto vía el simulador, como vía un *switch* real en laboratorio.

Actividad 1: Observe el arranque de un switch, y responda el cuestionario.

1. Indique el procesador empleado por el *switch*.
2. Indique la versión del IOS.
3. Indique la dirección MAC base del *switch.*
4. Indique la capacidad de la memoria *flash*.
5. Indique si el *switch* cuenta con fuente redundante.

Actividad 2: Vía simulador conecte cuatro *host* a un *switch* y acceda al mismo vía la consola, para asignar las "direcciones IP" y sus correspondientes "máscaras de subred natural" para cada *host*.

Actividad 3: Pruebe la conectividad entre *hosts* mediante paquetes PDU y *ping* enfocándose en entender el flujo de los paquetes ARP e ICMP y compruebe el llenado de las tablas ARP en los *hosts* y de la tabla MAC en el *switch*.

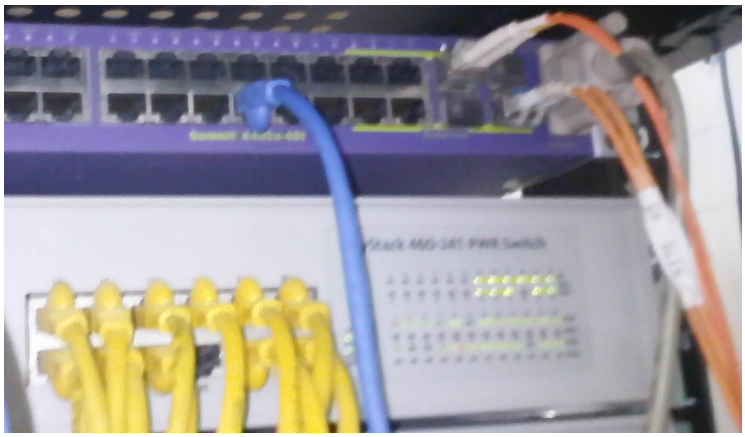
Actividad 4: Ingrese al *switch* para solicitarle su:

1. Versión del IOS
2. Usuarios
3. Contenido de la memoria *flash*
4. Hora
5. Detalles de sus interfaces
6. Contenido de la tabla MAC
7. Contenido de la tabla VLAN
8. Configuración que actualmente se está ejecutando

Actividad 5: Ingrese al *switch* para cambiar la configuración realizando:

1. Cambio del nombre del *switch*
2. Deshabilitación y habilitación de las interfaces del *switch*
3. Guardado de la configuración en la memoria *flash*
4. Otras instrucciones útiles para monitoreo son "show interfaces", "show arp" y show controllers". Practique con las versiones completas y versiones cortas de las órdenes.

Actividad 6: En la siguiente figura identifique, UTP y fibra óptica (FO) en los *switches Summit de Extreme Networks* y *Baystack de Nortel*.



II.5 Subredes: Configuración vía NIC

Dado el agotamiento de las direcciones de internet de IPv4 (32 bits), con sus 4.3 mil millones de direcciones, a partir del 6 de junio de 2012 se liberó el protocolo IPv6 (128 bits), y los proveedores de servicios de comunicaciones (CSP), así como los proveedores de servicios de internet (ISP) realizaron pruebas para este. Existe una gran preocupación, tanto de los CSP como de los ISP, sobre cómo prepararse cada vez mejor acerca de la forma en que trabajará IPv6, cómo convivirán en el futuro IPv4 e IPV6; y, si se usa infraestructura con IPv4, cómo se harían los túneles o técnicas de encapsulamiento con IPv6 hacia IPv4, etc. Por lo que, sin duda es importante revisar los detalles de implementación de IPv4 **[1]**.

¿Cómo se ha respondido en el pasado ante una crisis por agotamiento de direcciones IPV4?

Para un administrador de redes WAN o MAN es fundamental configurar las redes de modo que se pueda trabajar, de la manera más eficiente posible, el empleo de direcciones IP y el enrutamiento de los paquetes de Internet. En los inicios de Internet se creó el "enrutamiento por clases", en el que sólo se empleaban las típicas redes clase A, B o C. Sin embargo, el empleo de **subredes (*subneting*)** permite optimizar el uso de las redes, para lo cual cada clase de red cuenta con subredes cuyo número es fijo, usando la Dirección de la Máscara de Subred (S*ubnet Mask Address*) –en este caso hablamos de la máscara de subred natural, la cual no se debe confundir con la máscara de red natural–. Las **subredes** permiten crear múltiples redes lógicas que existen dentro de las redes de las clases A, B y C. En el caso de no usar las subredes, se tendrían disponibles las redes naturales, pero habría un gran desperdicio. Sólo como recordatorio, se muestran las tablas II.2 y II.3. La tabla II.2 muestra la clasificación de redes clase A, B, C, D y, la tabla II.3, el caso de las máscaras naturales, que nos indican que no se están usando subredes; y las máscaras de subred, que nos indican que se están usando subredes. En este caso se usa la misma máscara de subred para todas las subredes de la misma familia, por lo que cada subred tiene el mismo número de direcciones de *host* disponibles **[2]**.

Clase	Rango de direcciones IP públicas para hosts	Rango de direcciones IP privadas para hosts	Máscaras de subred "Natural"
A	**RED** . host . host . host $2^7 - 2 = 126$ Redes:	$2^{24} - 2 = 16{,}777{,}214$ host	255.0.0.0
	1.0.0.1 - **126**.255.255.254	**10**.0.0.1 - **10**.255.255.254	
B	**RED** . **RED** . host . host $2^{14} = 16{,}384$ Redes:	$2^{16} - 2 = 65{,}534$ host	255.255.0.0
	128.0.0.1 - **191.255**.255.254	**172**.16.0.1 - **172**.31.255.254	
C	**RED** . **RED** . **RED** . host $2^{21} = 2{,}097{,}152$ Redes:	$2^8 - 2 = 254$ host	255.255.255.0
	192.0.0.1 - **223.255.255**.254	**192**.168.0.1 - **192**.168.255.254	
D	**224.0.0.0 - 239.255.255.255**	**MULTICAST**	

Tabla II.2 Rango para las IP para *hosts* en redes de clases A, B, C y D.

Clase	Direcciones IP para red	Máscara natural de red	Direcciones IP	Máscara
	Sin subredes		Con subredes	
A	**10**.0.0.0	255.0.0.0	**10**.0.0.0	255.32.0.0
B	**150.40**.0.0	255.255.0.0	**150.40**.0.0	255.255.248.0
C	**200.80.120**.0	255.255.255.0	**200.80.120**.0	255.255.255.224

Tabla II.3 Ejemplos de redes clases A, B y C, sin subredes y con subredes.

Debe observarse que, en una determinada red o subred, a la NIC no se le asigna, como dirección IP, ni la primera dirección (por ser la dirección de la subred), por ejemplo 10.0.0.0; ni la última dirección (la cual se reserva para realizar *broadcast* dentro de la subred), por ejemplo 10.255.255.255.

El crecimiento exponencial en Internet generó la necesidad de no desperdiciar direcciones, razón por la que se creó el "enrutamiento sin clases", de modo que se crearon las subredes, mismas que tienen un número de host variables. Dada la importancia de las redes en la vida práctica, se abordarán a detalle **[1, 11]**.

Por lo anterior, en 1993, se creó el *Classless Inter Domain Routing* (CIDR), el cual usa la técnica *Variable Length Subnet Mask* (VLSM) que emplea máscaras de subred de longitud variable

para lograr que las tablas de enrutamiento no fuesen tan grandes y para permitir que, al usar de manera óptima las direcciones de Internet, se desacelerara la necesidad de las direcciones de IPv4. Este último tema queda fuera del alcance de esta obra, por lo que nos centraremos en comprender el funcionamiento de las subredes de clases A, B y C.

La tabla II.4 muestra los valores binarios para la máscara de subred y los valores decimales de las máscaras de subred en IPV4, así como el número de bits (x) empleado para subredes con base en el cual se calcula el número de subredes **[Ns=2^x-2]**; también se indican el número de bits (y) empleados para los *hosts*, con lo cual se calcula el número de *host* por subred **[Nhs=2^y-2]**.

A continuación, se revisan las subredes en la clase C, por ser el caso más sencillo de analizar. Una vez entendiendo éste, la obtención de las subredes de clases A y B se obtienen de manera similar [1].

Valores binarios para las distintas máscaras de subred	Valores decimales para las máscaras de subred	Bits para Subredes/ # Subredes	Bits para Host / # host x subred
11111111.11111111.11111111.00000000	255.255.255.000	Natural	
11111111.11111111.11111111.10000000	255.255.255.128	1/0	7/126
11111111.11111111.11111111.11000000	255.255.255.192	2/2	6/62
11111111.11111111.11111111.11100000	255.255.255.224	3/6	5/30
11111111.11111111.11111111.11110000	255.255.255.240	4/14	4/14
11111111.11111111.11111111.11111000	255.255.255.248	5/30	3/6
11111111.11111111.11111111.11111100	255.255.255.252	6/62	2/2
11111111.11111111.11111111.11111110	255.255.255.254	7/126	1/0
11111111.11111111.11111111.11111111	255.255.255.255	Difusión	

Tabla II.4 Máscaras de subred para la clase C en IPV4; cada una cuenta con un número fijo de subredes y con un número fijo de *hosts* por subred.

La figura II.17 muestra el diagrama usado para la simulación para las subredes 252 de clase C; observe sus 62 subredes, con 2 hosts cada una, para obtener un total de 124 hosts.

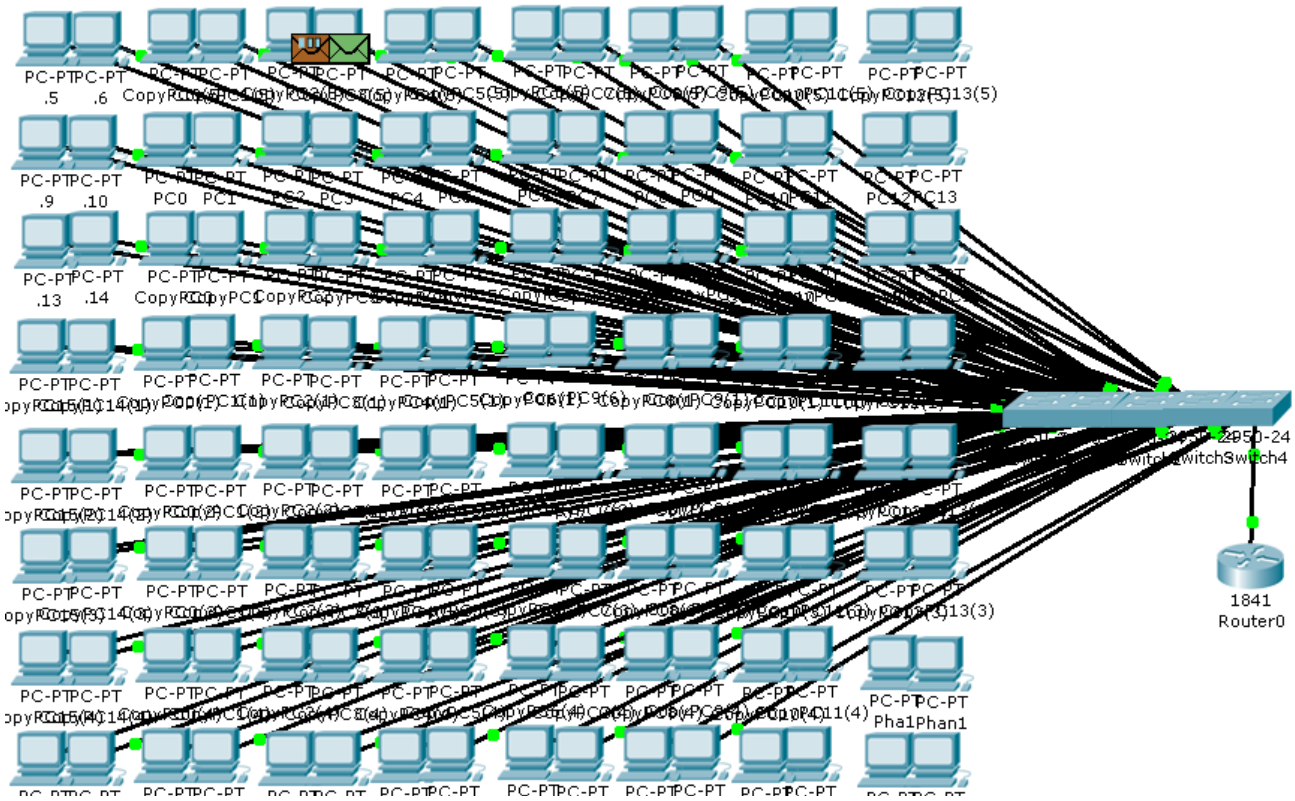


Fig. II.17. Subred 252 para la clase C.

La tabla II.5 compara el número total de *hosts* posibles sin usar subredes, contra el número total de *hosts* disponibles al utilizar subredes, por lo que resulta evidente la ventaja, en términos de un mayor número de *host* disponibles para una infraestructura determinada, cuando se usan subredes [1].

CLASE	***Hosts* sin usar subredes.**	***Hosts* al emplear subredes.**
A	$2^{24} = 16{,}777{,}216$	302,055,304
B	$2^{16} = 65{,}534$	720,964
C	$2^{8} = 256$	804

Tabla II.5 Comparativo al usar y no usar subredes

II.6 Subredes: Configuración vía *switch* - VLAN

Después del nacimiento comercial de Ethernet, en 1980, su gran aceptación en la misma década se debió a que proveía un medio de transporte compartido, en el que todos los equipos tenían comunicación con todos los demás equipos, quedando todos en un mismo dominio de ***broadcast***. El *switch* resolvió el problema de un mismo dominio de colisión que presentaban los *hubs*, y cada puerto del *switch* es un dominio de colisión; pero ahora todos los puertos quedan en un mismo dominio de *broadcast* –como ya se vio en los ejercicios prácticos–, cuando al enviar un ping, el proceso ARP o ICMP envía paquetes desde un *switch* hacia todas sus interfaces.

A mediados de los 90, se usó el estándar IEEE 802.1Q-1998 para introducir las VLAN, y crear redes LAN lógicamente independientes, al desagregar los dominios de ***broadcast*** sobre una red física simple, lo que fue definiendo las Clases de Servicio (*Class of Service* - CoS) y calidad en el servicio (*Quality of Service*- QoS). Para ello, se requirió modificar a la trama de Ethernet, agregando 32 bits para las etiquetas de las VLAN, los cuales fueron añadidos por los switches para identificar las VLAN de las tramas sobre los enlaces inter-*switches* **[11]**.

Un *switch* debe admitir y reenviar tramas sólo sobre los puertos que fueron configurados con el mismo identificador VLAN. Lo que motivó las VLAN fue proveer seguridad sobre una red física compartida, a través de la segregación de tráfico lógico y un uso del ancho de banda más eficiente, al limitar el alcance del tráfico ***broadcast*** o ***multicast*** (multidifusión) que inunda a una VLAN en lugar de hacerlo sobre la red física entera.

Los diseñadores concibieron VLAN de tamaño modesto, tal que algunos cientos de VLAN fueran suficientes, entonces agregaron 12 bits para el identificador VLAN, lo cual limitó el número de identificadores a 4094, ya que el 0 y 4095 quedaron reservados. Para crear una VLAN primero se genera una base de datos, después se crean las VLAN y, finalmente, se asignan cada uno de los puertos a las VLAN existentes en la base de datos.

En el caso de que se necesite expandir las VLAN se usa un trocal (***trunk***), el cual es un enlace punto a punto, entre uno o más puertos de *switches* y otro *switch* o *router*. Un *trunk* lleva el tráfico de muchas VLAN sobre un único enlace y permite extender las VLAN a través de toda una red. El tipo de encapsulamiento típico es el IEEE 802.1Q, pero también existen del tipo propietario, como el *Inter Switch Link Protocol* (ISL) de Cisco. Antes de usar *trunking,* se debe verificar que los *switches* o *routers* soporten tal funcionalidad y, en caso de necesitarlo, incluso habilitar el Protocolo Troncal Dinámico (*Dynamic Trunking Protocol* - DTP), el cual inhabilitará lógicamente puertos que pudiesen conducir a tormentas de *broadcast* **[11]**.

La figura II.18 muestra cómo se agrupan 3 VLANs y cómo, al enviar paquetes desde un miembro de una VLAN, al llegar al *switch*, solamente se hará vía la inundación tipo *broadcasting* dentro de la VLAN correspondiente. Por ejemplo, desde un equipo de contabilidad hacia su servidor de contabilidad ya que, de ninguna manera, un miembro de una VLAN podrá comunicarse con otro miembro que pertenezca a otra VLAN, proveyendo seguridad a nivel de "máquina real" o de nivel digital.

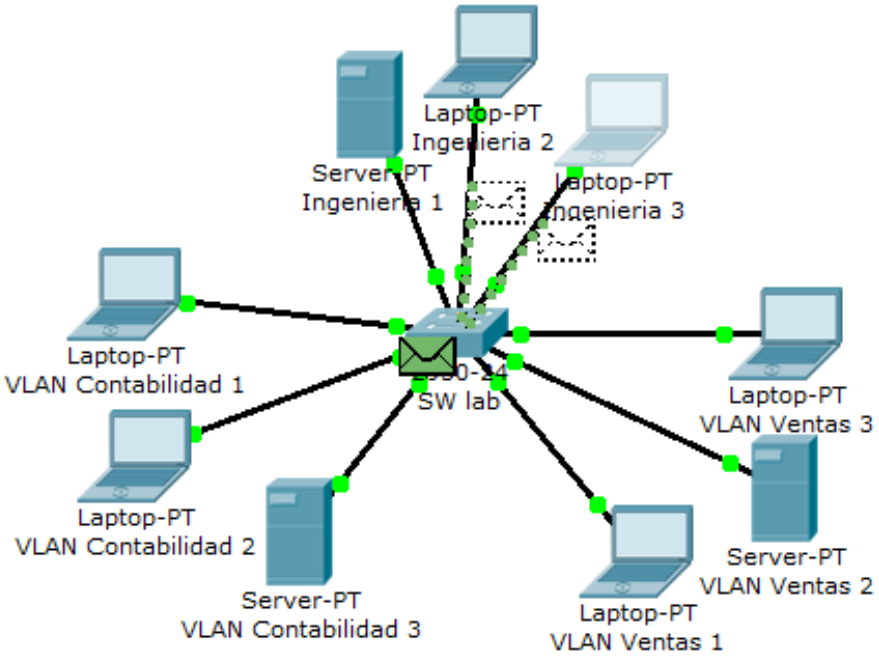


Fig. II.18 Tres VLAN construidas en una red.

Para la configuración de VLANs, deben seguirse básicamente 3 pasos:

1. **Crear la base de datos de las VLAN.** Por lo general ya están creadas, y se les puede verificar al monitorear y solicitar la tabla VLAN, vía el comando ***show vlan.***
2. **Crear las VLAN indicando su nombre y asociándolo a un número** de manera unívoca, ya sea usando la orden [switch(config)#**vlan** 5 **name** ingenieria)], o de manera gráfica vía una GUI, como se puede observar en la figura II.19, en la cual se muestra la base de datos de la VLAN ya creada, junto con las VLAN default y las reservadas. El borrado se hace con la orden [switch(config)#**vlan** 5] o, si lo prefiere, se puede sobre escribir.

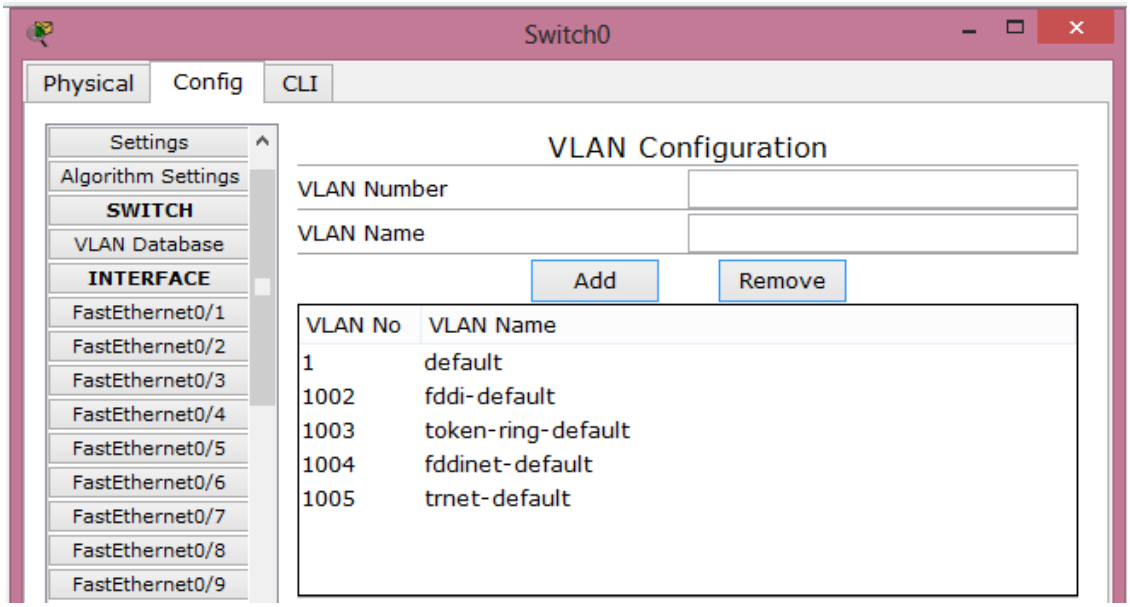


Fig. II.19 Ingresos a la base de datos de la VLAN para poder crear la VLAN.

Una vez creadas las VLAN, se verifica que no existan errores, como se indica en la figura II.20, donde se observan las nuevas VLAN. En este ejemplo, todas las 24 interfaces o puertos del switch están asignados a la VLAN 1 –la VLAN default–, lo cual indica que no existen VLAN activas.

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
5    Ingenieria                        active
10   Contabilidad                      active
20   Ventas                            active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Fig. II.20 La base de datos muestra que se han creado 3 nuevas VLAN.

3. **Asignación de puertos a una VLAN:** En este ejemplo, las interfaces 1, 2, 3 se asignan a la VLAN de "ingeniería"; las interfaces 4, 5, 6 a la VLAN de "contabilidad" y las interfaces 7, 8 y 9 a la VLAN de "ventas". Primero se elige una interfaz y luego esta se asigna a un puerto del *switch*, por medio del **modo acceso**. Por ejemplo, para asignar un puerto a la VLAN 5 se procede como sigue:

[switch(config)#**interface fa0/1]**
[switch(config-if)#switchport access vlan 5**]**

Los resultados se verifican en la figura II.21, de manera que se logran los resultados indicados en la figura II.18.

```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
5    Ingenieria                       active    Fa0/1, Fa0/2, Fa0/3
10   Contabilidad                     active    Fa0/4, Fa0/5, Fa0/6
20   Ventas                           active    Fa0/7, Fa0/8, Fa0/9
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Fig. II.21 La base de datos muestra que se han asignado los puertos correctamente a cada VLAN.

Ahora, ¿qué sucede si sólo se cuenta con un número limitado de interfaces en un *switch* y se desea que cada VLAN tenga un número mayor de *hosts* al de la capacidad de un *switch*?

II.6.1 Modo Troncal

Entonces se deben crear las VLAN en 2 o más *switches*, para hacer el equivalente a una expansión de VLAN. Para ello, los *switches* deberán interconectarse bajo el ***modo trunk,*** para indicar que ésta es la vía de salida al otro *switch*, donde está la otra parte de los miembros de una VLAN, lo cual se puede configurar de la siguiente manera:

[switch(config)#**interface fa0/24]**

[switch(config-if)#switchport mode trunk**]**

El resultado es que el circuito de las VLAN opera con dos *switches*, como se indica en la figura II.22 **[1, 11]**.

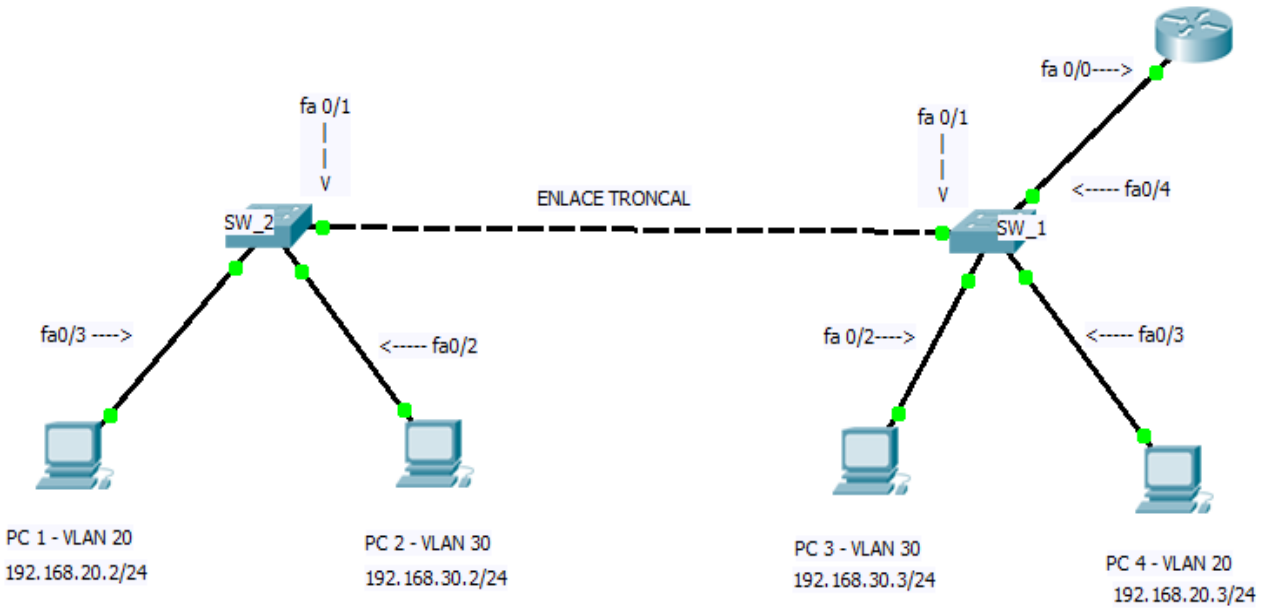


Fig. II.22 VLAN construidas en una red, mediante la conexión de 2 *switches* vía *trunk*.

Finalmente, a manera de resumen, se presenta el "caligrama con forma de switch" como se indica en la figura II.23.

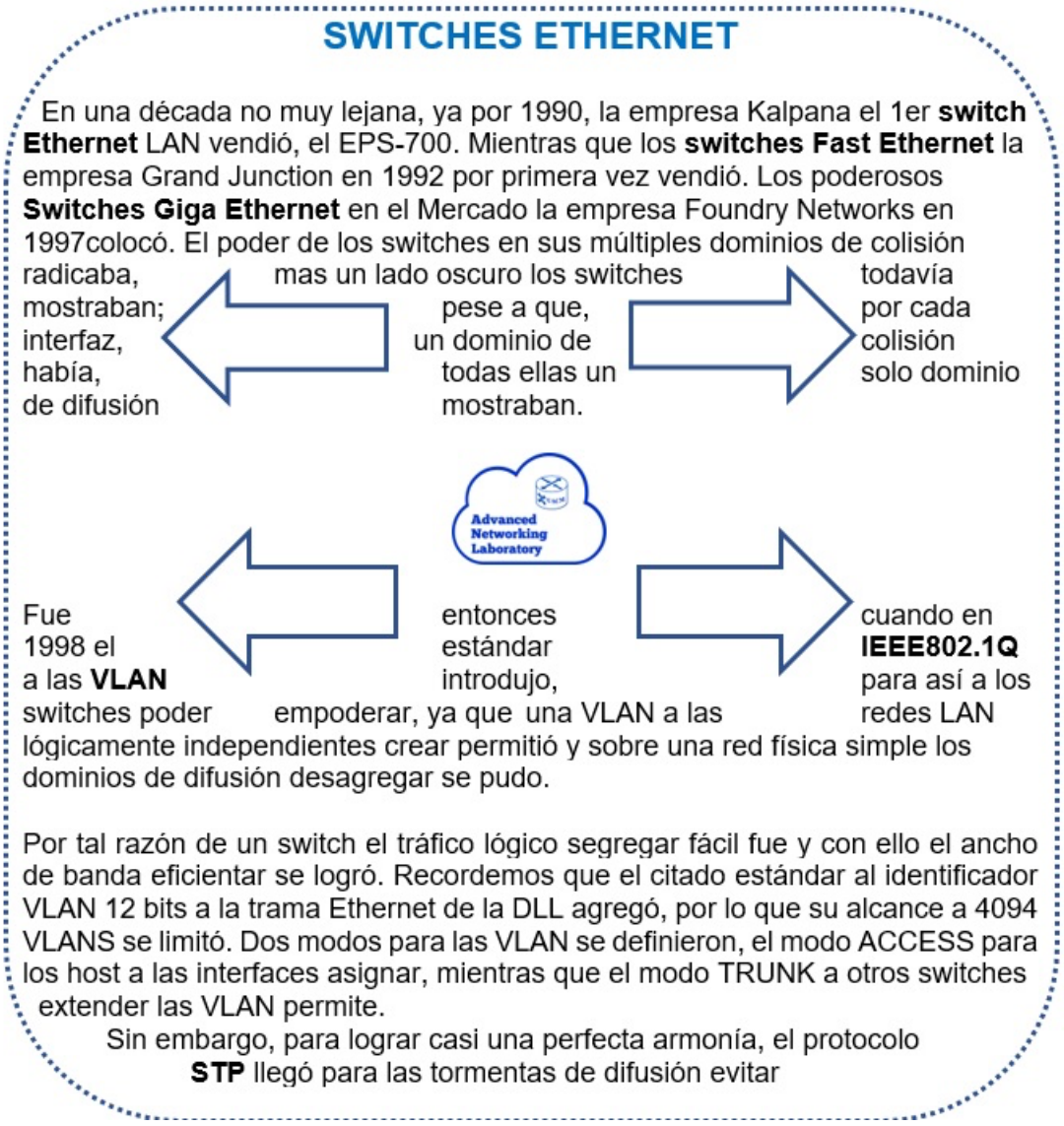


Fig. II.23 Resumen de la tecnología *switch* Ethernet mediante un caligrama.

IV.7 PRÁCTICA 3: Subredes vía NIC y vía switch

El objetivo de esta práctica es simular la creación de subredes, ya sea vía *subneting* configurando cada NIC en una red, o creando VLANs en un *switch*.

Actividad 1-*Subnetting*.

De las 5 familias de Subredes para las redes de clase C, realice la simulación completa de una de ellas.

Actividad 2-VLAN con un *switch*

Suponga que se encuentra en una empresa y le solicitan que genere 6 VLAN, con un *switch* que tiene 24 interfaces, y que a cada VLAN le asigne 4 *hosts,* incluyendo a un servidor por VLAN.

Actividad 3-VLAN con dos *switches*

Suponga que se encuentra en una empresa y le solicitan que genere 6 VLAN con 6 *hosts,* cada una incluyendo a un servidor por VLAN. Considere que usted sólo cuenta con *switches* de 24 interfaces.

IV.8 EVALUACIÓN PARTE I

De acuerdo con la taxonomía de Bloom, de los 6 niveles de pensamiento, los 3 primeros se denominan los niveles de pensamiento inferior en el dominio cognitivo. En esta evaluación se cubren los 2 primeros, [1p] conocer (recordar) y [2p] entender (comprender), mientras que el tercero [3p] aplicar se cubre al evaluar las prácticas de laboratorio y los reportes de cada estudiante. La evaluación consta de 3 secciones para un total de 20 puntos.

I. SECCIÓN A: *Switching* básico

1. **Describa** la función de un *hub* y de un *switch* indicando las capas del modelo ISO/OSI en las que opera [1p]

_____

_____

_____

2. **Indique** los estándares que marcaron el inicio, en 1990, (encierre en un óvalo) y fin, en 1999, (subraye) del empleo de los *hubs Ethernet* [1p].

A) A. 10BASE5
B) B. 10BASE2
C) C. 10BASET
D) D. 100BASETX
E) E. 1000BASET
F) F. 1000BASEFB
G) G. 10GE
H) H. 40GE

3. Cuando un *switch* recibe una trama *unicast,* por una de sus interfaces, realiza un proceso y toma una decisión. **Enuncie** las opciones que tiene por hacer, con la trama recibida, y en qué consisten [1p]:

A)_____

B)_____

4. **Indique** el nombre una serie de SW Cisco por categoría [1p]

Switch	Familia
Para "SOHO" (Ejemplo)	Catalyst 1548 Micro
Para "acceso"	
Para "acceso"	
Para "*backbone*"	

5. **Defina** detalladamente "topología de red" [1p]

_____

_____

_____

6. Considere dos LAN, una creada con un *hub* y otra con un *switch, entonces* [1p]*:*
   A) Indique la diferencia, entre ambas, al enviar paquetes de manera simultánea entre todos los *hosts* de la LAN.
   B) Indique el número de dominios de colisión para cada caso.
   C) Indique qué sucede con el ancho de banda del canal que usa un *hub*.

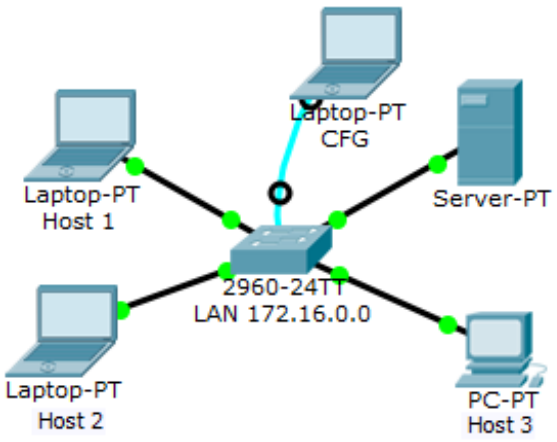
_____

_____

_____

_____

7. A partir de la siguiente figura de LAN básica, asigne las "direcciones IP" y sus correspondientes "máscaras de subred natural" para cada *end system* en la LAN, para ello, llene la tabla ARP *[1p]*
8. Asigne las interfaces para el *switch* y llene la tabla MAC indicando los encabezados [1p]



Tablas ARP en cada NIC		
HOST	IP Address	Subnet Mask
Host 1		
Host 2		
Host 3		
Server		

9. ¿Es necesario indicar la dirección IP del *gateway* en cada NIC? SI o NO, R: _____ **Justifique** su respuesta [1p]:

Tabla MAC			
VLAN	MAC ADDRESS	TYPE	PORT

10. El estándar IEEE 802.3 [Ethernet II] se fundamenta en el proceso CSMA/CD. Expandir las siglas y explicar los procesos [1p]

_____

_____

_____

II. SECCIÓN B: Monitoreo y configuración básicos

1. **Indique** el procedimiento que usted debe seguir, paso a paso, (completando los espacios correspondientes) para habilitar a la interfaz *Fast* Ethernet conectada al *host* 1 de la figura 1. [2p].

Lab>_____

Lab#_____

One command per line. Ctrl Z to exit

Lab(Conf)#_____

Lab(Conf-Int)#_____

%LINK5-CHANGED: Interface FastEthernet ____, changed state to administratively up.

2. Una vez que la LAN se encuentra operativa, **indique** el procedimiento que usted siguió, paso a paso, (completando los espacios correspondientes) para obtener la tabla MAC [1p]

Lab#_____

3. Dada una LAN en la que las interfaces de los *switches* y NICs de sus *hosts* son Giga Ethernet, **mencione** el estándar IEEE el cual indica que debe usarse, como mínimo, un cable cuya categoría soporte "1000 Base-T" [1p]

_____

III. SECCIÓN C: Subredes

1. Dada la subred 255.255.255.248, configurada vía NIC [2p].
   A) **Indique** el número de subredes máximo_____
   Justifique_____
   B) **Señale** el número de *host*s por subred_____
   Justifique_____
2. **Mencione** el estándar que permitió introducir las VLAN en 1998 [1p]

_____

3. **Diga** cuál es el objetivo de las VLAN [1p]

_____

_____

4. **Enuncie** el número máximo de VLANS que se pueden crear en un *switch* y cuál es el motivo indicado en el estándar [1p]

_____

_____

5. **Señale** la diferencia entre las funciones de los modos **access** y **trunk** en un switch [1p]

_____

_____

_____

PARTE II: ENRUTAMIENTO

CAPÍTULO III: ENRUTAMIENTO ESTÁTICO

Mientras había pocas redes y los equipos de interconexión no existían en grandes cantidades, la manera de indicar desde dónde nos estamos conectando hasta el destino se hacía de manera manual. Para ello los administradores de red necesitaban conocer la topología de toda la red, con la complejidad que ello conllevaba. Por su parte, los equipos que realizaban la conmutación, a nivel de enrutamiento evolucionaron de IMP a *gateways* y de allí a *routers*.

III.1 IMP, *gateway* y *router*

En el principio de ARPANET, y hasta 1973, se emplearon Procesadores de Mensajes de Interfaz (*Interfaz Message Processors* - IMP), los cuales eran minicomputadoras Honeywell DDP-316 que se conectaban a la PSTN a 56 Kbps.

Desde 1973 se usaron *gateways* **[12]**. En noviembre de 1994, se hizo imperante clarificar la diferencia entre *gateways* y *routers,* mediante el documento: "*Towards requirements for IP routers",* en el que se destacaban 4 hechos **[13]**:

1) Era común llamar *gateways* a los *routers* en todos los documentos anteriores a 1994.

2) Los *routers* eran computadoras de propósito general, que ejecutaban específicamente *software* para conmutación de paquetes.

3) Internet (todavía NSFNET) era una red de redes, cuya interconexión ya presentaba un crecimiento exponencial **[14]**.

4) Conforme se evolucionaba, los *routers se implementaban* en computadoras para aplicaciones generales y, luego, se fueron convirtiendo en computadoras específicas, tal como ocurrió con los microcontroladores para hornos de microondas, refrigeradores, motocicletas, autos, drones, etc., para hacer a los equipos un poco más económicos.

Entonces fue necesario hacer actualizaciones, dadas las dificultades en la administración de la red. Un *router,* o enrutador, interconecta 2 o más redes y elige el mejor de los caminos o rutas entre las redes. Toda la información acerca de las posibles rutas en la red se almacena en una de las **bases de datos** de cada *router,* en este caso, a la que conocemos como **tabla de enrutamiento.** En esta época las LAN tenían velocidades de 10 Mbps y las pocas LAN existentes con base en fibra óptica (FDDI) tenían velocidades de 100 Mbps, por lo que los llamados ***embedded routers*** (es decir, computadoras para aplicaciones específicas de ruteo) eran ya una necesidad, considerando que muchas de las líneas que permitían conectarse a Internet tenían velocidades de 56 kbps (DS0), 1.4 Mbps (DS1) o 45 Mbps (DS3). En 1995, se especificaron los requerimientos para el uso de *routers* bajo el protocolo IPV4 **[15]**. La evolución, desde IMP, a *routers* se puede apreciar en la parte inferior de la figura I.1

En la figura III.1, se muestra la topología de una red casera que conecta a un *host* con un servidor en la Internet, mediante un equipo de dimensiones reducidas, el cual puede ser del tipo 5 en 1 (*router, modem, switch, firewall y access point*). En una vivienda, café internet, microempresa, escuela o área de trabajo, seguramente, habrá una red LAN. Para que una computadora se conecte

a la LAN, el equipo que hace las funciones de *modem, router, switch y access point* permitirá conectase a la red mediante una determinada NIC o WNIC en la computadora, es decir, vía Ethernet mediante IEEE 802.3 o vía WiFi por medio de IEEE 802.11.

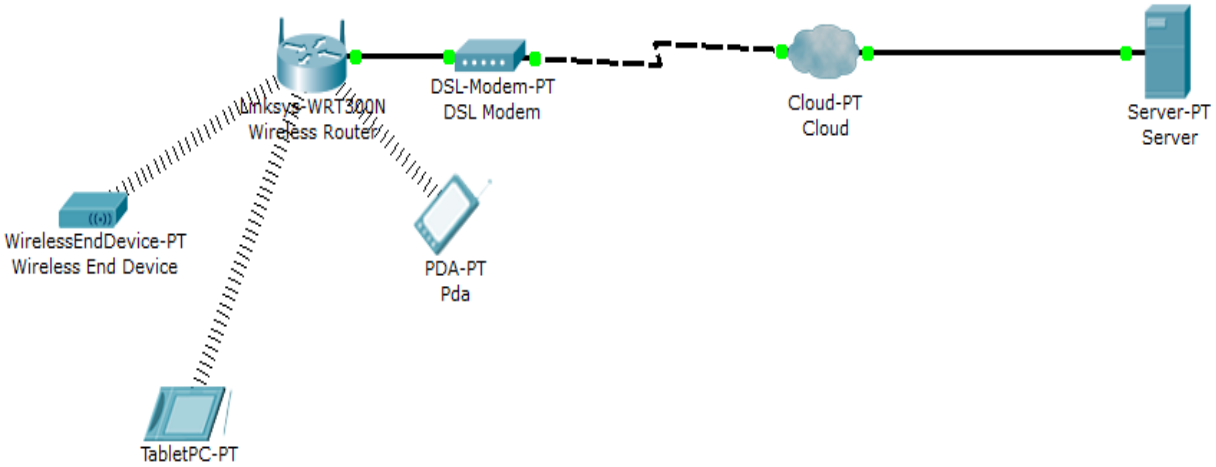


Fig. III.1. Conexión desde casa o café internet con un servidor en la internet.

Cada equipo *host* debe contar, al menos, con una NIC o una WNIC, la cual tiene asociada una dirección física, a la que, ya sea manualmente o vía un Protocolo de configuración dinámica para *hosts* (*Dynamic Host Configuration Protocol* - DHCP), se le asignará una dirección lógica, como lo muestra la figura III.2.

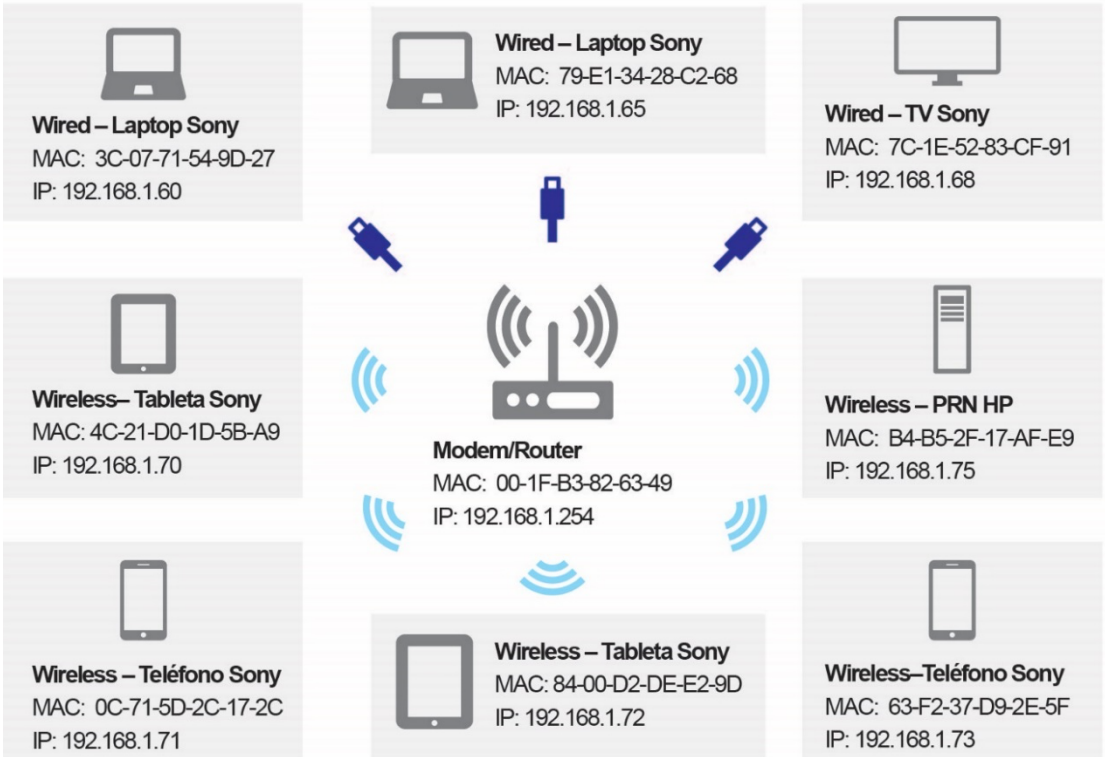


Fig. III.2 Topología de una red casera típica en la que conviven *end systems* vía Ethernet y Wifi.

En la figura III.2 también observamos distintas conexiones para cables. Aun cuando los equipos en la actualidad permiten la identificación automática del tipo de cable empleado, es recomendable conocer los cables necesarios, ya sea del tipo recto (*straight through*) o cruzado (*crossover*). Si un *router* se emplea en una red para datos con servicios de doble *play* (telefonía e internet), triple *play* (telefonía, internet y video) o tetra *play* (triple *play* más telefonía celular), las tareas básicas con un *router* son las mismas.

Las operaciones, que a continuación realizaremos, son aplicables tanto si los *routers* empleados son del tipo acceso, para unir 2 LAN pequeñas, o si son del tipo núcleo o *core*, que forman parte del *backbone* de un Proveedor de Servicios de Internet (*Internet Service Provider* - ISP); es decir, la forma en cómo nos comunicaremos con un *router* de Cisco será similar a la forma en cómo nos comunicaremos con un *router* Juniper, Lucent Alcatel, Alcatel-Lucent, Nortel, 3COM, Huawei, etc.

En 2008 con la crisis económica global, generada desde EUA, las empresas 3COM de EUA (1979-2010) y Nortel de Canadá (1895-2009) quebraron rotundamente y, como todo en el universo, la muerte de unos es el alimento de otros; en este caso el personal y tecnología fueron incorporadas a otras empresas. Algo similar sucedió, con Alcatel y Lucent, para crear Alcatel-Lucent **[1]**.

En el caso de los *routers* de Cisco, como bien sabemos, existen las familias de las series 2600, 3600, 3800, 7200, 7500, AS5800, 10000 y 12000 (donde los dos últimos podrían dar soporte a aproximadamente 100,000 clientes cada uno). Los diferentes modelos tienen aplicación en distintas áreas de una red, es decir, algunos funcionan como *routers* de ***backbone*** (similares a las carreteras principales) y otros se prefieren para el **nivel de distribución** (similares a las carreteras secundarias) y de allí hasta llegar a los corporativos, empresas, bancos, universidades, hogares, etc. **[1]**.

La figura III.3 muestra algunos modelos Cisco de tipo acceso, pese a que algunos ya están considerados como obsoletos, dado que el mercado global está inundado de millones de ellos en funcionamiento y los simuladores lo soportan; de modo que, para aprender y practicar, siguen siendo vigentes.

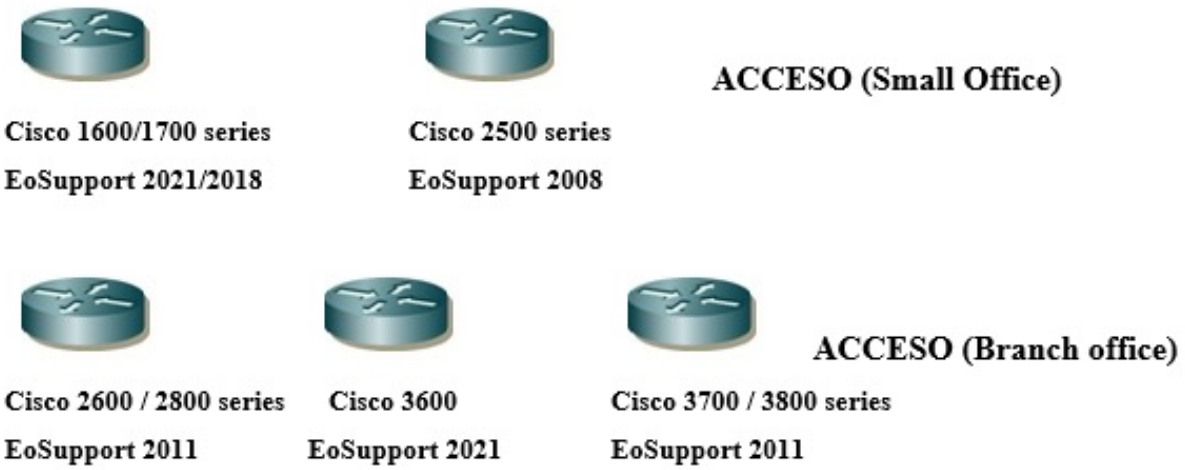
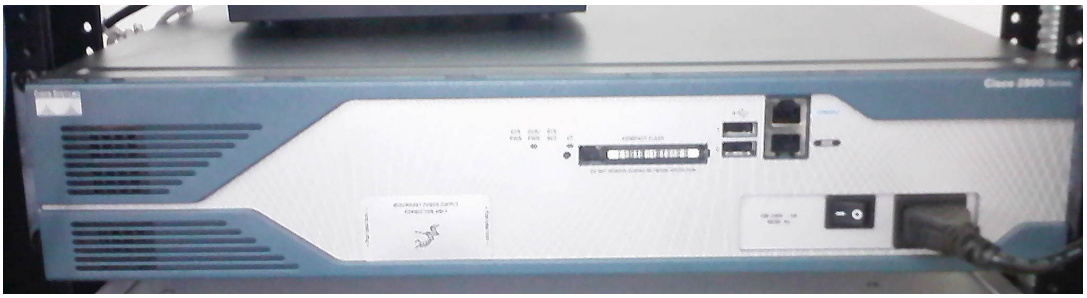


Fig. III.3 Gama de *routers* de acceso Cisco. Para prácticas se recomienda al menos la familia 2600.

La apariencia física de un *router* de acceso marca Cisco se muestra en la figura III.4A. En la figura III4B se muestra, parcialmente, un rack. Observe al *router* con fuente redundante.



A

B

Fig. III.4. A) Un *router* de acceso Cisco 3845. B) Un *Router* Cisco con fuente redundante en un rack.

III.1.1 Ciclo de vida para *switches y routers*

La tabla III.1, resume el ciclo de vida de un *router* comercial Cisco del tipo acceso y, la tabla III.2, el correspondiente a un *router* Cisco del tipo núcleo o *core*.

Introduction year	1997 (Motorola 68030 20 MHz RISC, RAM: 4 MB, *memoria flash*: 4 MB (instalados) / 4 MB (máx.) / 10Mbps
EOS - End of Sale	December 14, 2001
EOHS - End of hardware support	April 30, 2004
ESS - End of software support	December 14, 2006
Product obsolescence/end of TAC support	December 14, 2007
EOS product:	Replacement product:
C 3810	C 2600 Series

Tabla III.1 Ciclo de vida para un *router* C3810.

Introduction year	2008 (Power Pc 667 MHz, RAM: 512 MB, *memoria flash*: 64 MB (instalados)
EOS - End of Sale	June 14, 2015
EOHS - End of hardware support	June 15, 2019
ESS - End of software support	December 15, 2020
Product obsolescence/end of TAC support	December 14, 2007
EOS product:	Replacement product:
C 12004	

Tabla III.2 Ciclo de vida para un *router* C12000.

Se recomienda que el lector obtenga tablas similares a III.1 y III.2 para *routers* de Cisco de la serie 3800, 7200, 10000 y 12000. También es deseable que busque de otros fabricantes, tanto *routers* de acceso como de distribución como los *core* o núcleo, usados como *Service Provider Edge* (PE *Router*).

Trate de responder a las preguntas: ¿Cuándo se declara a un *switch* o *router* como obsoleto? ¿Qué implicaciones tiene su obsolescencia en términos de su funcionamiento?

La figura III.5 muestra un caligrama correspondiente al *router* Ethernet a manera de resumen.

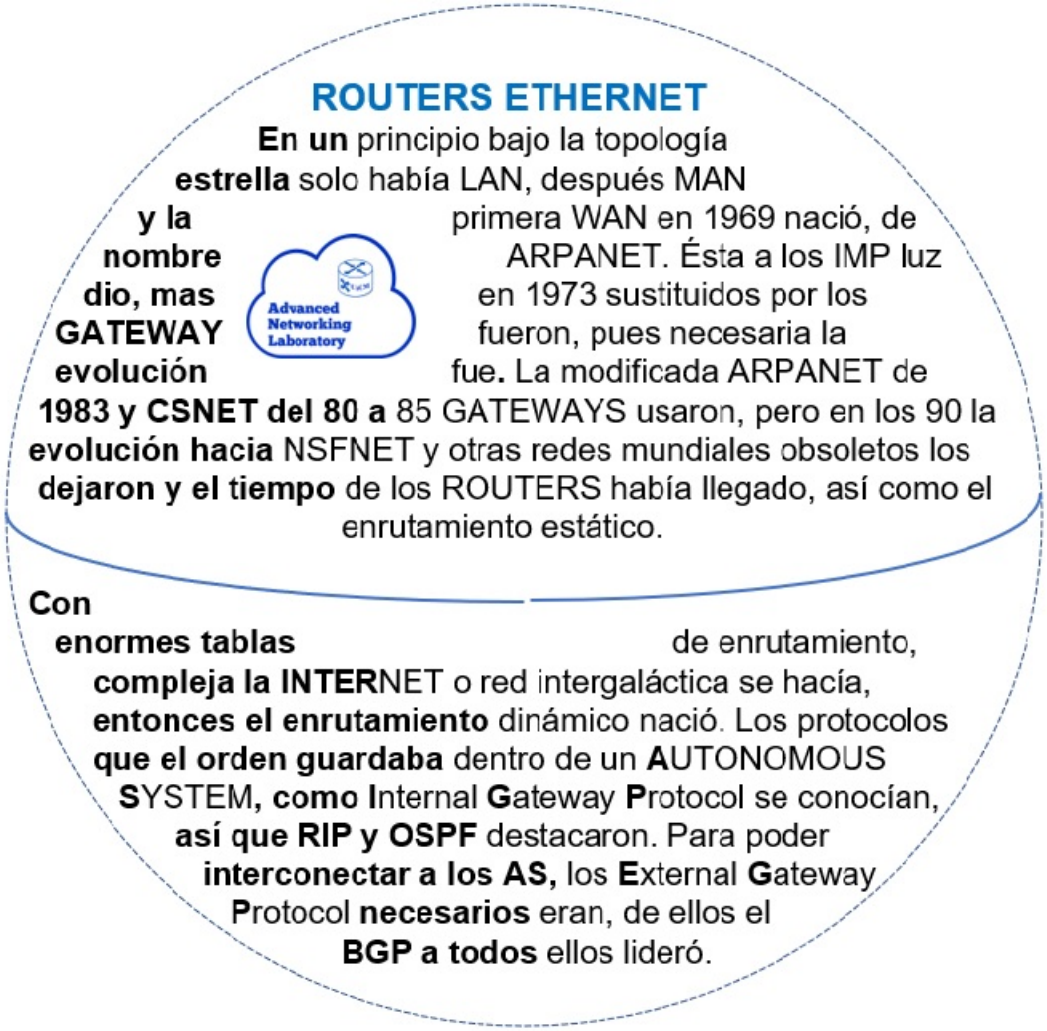


Fig. III.5 Resumen de la tecnología *router* Ethernet mediante un caligrama.

III.2 Arranque de un *router*

Un *router* es una computadora de propósito específico, especializada en aplicaciones para telecomunicaciones, en particular para redes de datos, cuyo arranque es similar al de una computadora genérica. Una vez que se arranca un *router,* se ejecutan, tanto el programa de inicialización como las pruebas POST; finalmente el *Internetworking Operative System (*IOS) toma el control del sistema, como se indica en la figura III.6

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by Cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Self decompressing the image:
################################################################################ [OK]
          Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software – Restricted Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.
        Cisco Systems, Inc.
        170 West Tasman Drive
        San Jose, California 95134-1706
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
Image text-base: 0x400A925C, database: 0x4372CE20
This product contains cryptographic features and is subject to United States and local country laws governing import,
export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors, and users are responsible for compliance with
U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance, please contact us by sending email to export@cisco.com.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
      --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>
```

Fig. III.6 Arranque de un *router* de acceso Cisco

Al igual que sucede con un *switch*, ya sea en el simulador o en un entorno real, se debe conectar un equipo que preste su teclado y monitor al *router* que se desea monitorear y configurar, como se indica en la figura III.7

Fig. III.7. Conexión de PC a consola vía cable de consola.

Para un *router* se sigue el mismo procedimiento que se mostró en la sección II.3, para un *switch,* a fin de interconectar la interfaz GUI que permitirá comunicarse con el *router*. Una vez que nos encontramos dentro del *router*, podemos conocer cuál es la versión del sistema operativo con el que ese *router* trabaja. La orden que nos permite conocer esa información es ***show versión*** y en la figura III.8 se indica el resultado de la petición.

```
router_prestado>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(5)T8, RELEASE SOFTWARE (fcl)
TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=support
Copyright (c) 1986-2001 by Cisco Systems, Inc.
Compiled Mon 07-may-01 by 17:57 xyz
Image text-base: 0x80008088, data-base:0x80972320
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fcl)
ROM: c2600 software (C2600-I-M), Version 12.1(5)T8, RELEASE SOFTWARE (fcl)
Router uptime is 3 days, 15 hours, 10 minutes
System returned to ROM by reload
System image file is “flash:c2600-i-mz.121-5.T8”
Cisco 2610 (MPC860) processor (revision 0x203) with 61440K/4096K
bytes of memory.
Processor board ID JAD06090J4A (2134577719)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial (sync/async) network interface(s)
32K bytes of non-volatile configuration memory
16384K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

Fig. III.8 Respuesta a la petición de la versión del sistema operativo usado por un *router* cisco 2600.

Observamos que se indica lo siguiente:

1. Que IOS es el sistema operativo del *router.*
2. El modelo de *router* empleado, un C2600.
3. La versión del sistema de arranque en ROM.
4. El tiempo que lleva encendido el *router.*
5. Cuál es el respaldo de arranque vía una memoria *flash.*
6. Modelo de la tarjeta madre y del procesador principal.
7. Interfaces básicas.
8. Cantidad de memoria *flash* exclusiva para el procesador.

Suponga, por otro lado, que contamos con un *router* marca Cisco. Consideremos que podemos acceder a él, de manera local mediante la consola, es decir, conectando directamente una computadora al puerto auxiliar o de consola, indicado en el propio *router* o de manera remota vía una conexión desde un servidor Unix, por ejemplo, o incluso desde una PC. Para acceder al *router* vía remota podemos emplear la orden ***telnet.*** Y si, además, queremos ingresar en el modo de administrador, con todos los privilegios, empleamos la orden ***enable***; el resultado de tal tarea se cumple de acuerdo con la figura III.9.

```
Servidor _lab#telnet 10.25.15.10
Trying 10.25.15.10…
Connected to 10.25.15.10.
Escape character is ´^]´.
User Access Verification
Username: dreamer
Password: pr3st4d0
router_prestado>enable
Password: prestado2010
router_prestado#
```

Fig. III.9 Conexión a un *router* vía remota desde un servidor.

III.3 Microprocesadores y nanoprocesadores empleados en *routers* y *switches*

En 1950, con la venta de la primera computadora comercial y con la llegada del transistor de silicio comercial, surgió la tercera revolución industrial de la electrónica de semiconductores.

En 1971 nació la **microelectrónica** con los primeros microprocesadores i4004, cuyos transistores eran de 10 micras y, en 1985, el i386 ya tenía transistores de 1 micra. En este punto, es importante recordar las secciones introductorias a microprocesadores y microcontroladores, en las décadas de los años 70 y 80 de la referencia 1.

En 1999, los *routers* de acceso, de la serie 700 de Cisco, tenían integrado un *hub* de 4 puertos; los *routers* emplearon procesadores **80386** a 25 Mhz, con 1MB de memoria *flash* y con interfaz 10 Base T **[1]**.

Entre 1993 y 2001, Cisco liberó al mercado sus *routers* de la serie 2500, los cuales se usaron para conectar redes Ethernet o Token Ring, vía la Red Digital de Servicios Integrados (*Integrated Services Digital Network* - ISDN), *Frame Relay* o E1, para pequeñas y medianas empresas. Tales *routers* emplearon al procesador Motorola **MC68EC030,** de arquitectura Harvard de 32 bits a 20 Mhz, para direccionar un máximo de 16MB. La serie 2500 fue sustituida por la serie 2600, con *routers* de acceso con conexiones LAN y WAN.

Durante la década de los años 90, algunas compañías que producían procesadores, hicieron adaptaciones de sus microprocesadores y produjeron versiones económicas para emplearlas como microcontroladores; tal es el caso de Motorola, la cual sacó al mercado las versiones EC (*Embedded Controller*), a partir de sus versiones de procesador –por ejemplo los MC68EC020, MC68EC030 y MC68EC040, a partir de los procesadores MC68020, MC68030 y MC68040 respectivamente–, así como, en el caso de Intel, los procesadores SX o Pentium Celeron son una versión económica de las series DX y Pentium. Para el caso de los *switches* Cisco, en sus modelos 2900, 2948G, 2980G, 4000,4050, 5000, 5500, 6000, 6500 y 7600, se emplea como tarjeta principal el *Supervisor Engine I*, la cual utiliza el procesador **MC68EC040** **[1]**.

Cisco emplea para sus *switches* y *routers* procesadores MIPS, todos con arquitectura RISC; por ejemplo, para el *Supervisor Engine II y II+,* ocupa el MIPS R4700 para sus modelos 2926, 4000, 4500, 5000, 5500, 6000, 6500 y 7600. Y de manera más reciente, Cisco usa un sistema llamado *CEF-Cisco Express Forwarding*, una tecnología de conmutación en capa 3, empleada para *routers* de la serie 7200 y 7500 en el nivel de núcleo, con la finalidad de que se mejore el desempeño de Internet. En los equipos más avanzados de Cisco, sus *routers* 10000 y 12000 GPR (*Gigabit Route*

Processor), empleados como *backbone* para Internet, se usan los procesadores R5000, con procesador MIPS IV de 64 bits, cuya primera versión se liberó en 1996.

En 2008, los procesadores contaban con transistores de 45nm, mientras que entre 2010 y 2011, se comercializaron los procesadores de 32 nm y, entre 2012 y 2013, los de 22 nm.

Para 2014 y 2015, se comercializaron los primeros procesadores iCORE M, cuyos transistores eran de 14 nm. Las memorias de 16 nm se comercializaron desde 2016, no así los procesadores.

En sentido estricto, los procesadores de 10 nm marcan formalmente el nacimiento de la *nanoelectrónica*, claro está, desde el punto de vista comercial y para poder decir, con toda justicia: "ya tenemos en nuestras computadoras nanoprocesadores" **[1]**. Actualmente, se siguen desarrollando mejores procesadores con mayor complejidad, incluso ante la limitación empírica de la ley de Moore de 1965 (la densidad de transistores se duplica cada 18 meses). Consulte los detalles hasta 2019 en la referencia **[2]**.

En 2020, se hicieron comerciales los nanoprocesadores de 10 nm y, en 2021, de 7 nm; de esta manera, la nanoelectrónica estaría alcanzándose a casi 50 años de la creación de la microelectrónica.

En 2022 están disponibles memorias de 5 nm, pero la comercialización de procesadores de esa escala estará por liberarse comercialmente en breve, mientras la guerra por los chips continua entre EUA y China, teniendo a Taiwán en medio de la disputa y las nuevas inversiones en plantas de semiconductores en Arizona EUA.

III.4 Circuito con base en un *router*: monitoreo y configuración básicas

Un *router* tiene como función interconectar dos o más redes. La figura III.10 muestra el circuito de red en el que se interconectan dos redes LAN. Lo que debemos tener claro es cómo habilitamos la conectividad entre las dos redes. Si, de entrada, suponemos que las redes acaban de conectarse, entonces partimos de condiciones iniciales, es decir, con las tablas MAC de ambos *switches* y la tabla de ruteo del *router* vacías.

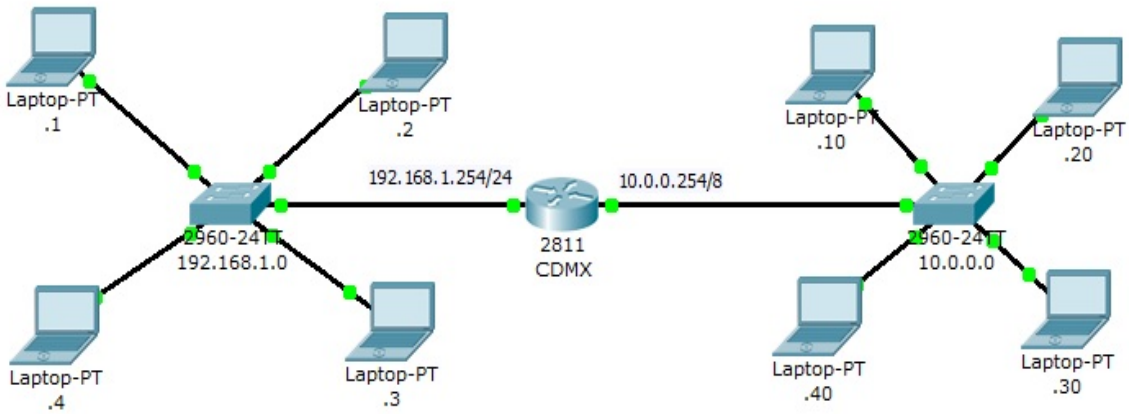


Fig. III.10 Circuito de red que interconecta dos redes mediante un *router*.

También debemos tener claro cómo es que un paquete sale de una red y cómo se va llenando la tabla MAC de su correspondiente *switch*, así como el camino que sigue para salir de la red, vía su dirección de *gateway*; es decir, la dirección de la interfaz del *router,* el cual pertenece a la misma red. Después, debe considerarse que, tanto la tabla ARP, en el *router*, como su tabla de enrutamiento, tienen registradas a las redes en cuestión. Finalmente, se debe entender cómo es que el paquete viaja hasta la otra red y llega hasta el *host* destino. Para obtener las tablas ARP y de enrutamiento, se usan las órdenes "*show arp*" y "*show ip route*", respectivamente. Observe que, una vez que las dos redes se conectan mediante el *router* empleando sus interfaces, **no se requiere de configuración alguna en el *router*,** ya que estas redes le son contiguas y el *router* las identifica automáticamente, como se puede constatar en la figura III.11, en la que se muestran las tablas ARP y de enrutamiento del *router*, respectivamente.

```
CDMX#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.254              -   0060.3E42.7502  ARPA   FastEthernet0/1
Internet  192.168.1.254           -   0060.3E42.7501  ARPA   FastEthernet0/0
CDMX#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
CDMX#
```

Fig. III.11 Tabla ARP y tabla de enrutamiento del *router*, con sólo 2 redes.

III.5 Interconexión de redes mediante enrutamiento estático

Un *router* interconecta redes y, para ello, envía paquetes entre redes, buscando en su tabla de ruteo y descubriendo cómo llega a redes remotas. La tabla de ruteo de cada *router* debe tener la dirección de los otros *routers* hacia dónde dirigir sus paquetes; en caso contrario, el *router* simplemente descartará los paquetes que reciba. Si una red en la que un *router* se conecta con otros *routers* vecinos, las redes contiguas se dan de alta en la tabla de enrutamiento automáticamente, (identificándolas con la letra C). Sin embargo, cuando una red es mediana o grande, se aplican dos diferentes tipos de enrutamiento: estático y dinámico. En el **enrutamiento estático,** un administrador de red se encarga de dar de alta, manualmente, las redes en cada una de las tablas de enrutamiento de los distintos *routers* que componen un determinado sistema. Este tipo de enrutamiento tiene las ventajas y desventajas indicadas en la tabla III.3 [1].

Ventajas	Desventajas
No hay sobrecarga en el CPU del *router.*	El administrador de red debe entender la interconexión de red para configurar correctamente cada *router*.
No hay uso de ancho de banda entre *routers.*	Al agregarse una nueva red a la interred, el administrador de red debe agregar esa nueva ruta en todos los *routers*.
Alta seguridad (sólo el administrador conoce las rutas).	En redes de gran tamaño actualizar las tablas de *routeo* es impráctico.

Tabla III.3. Ventajas y desventajas del enrutamiento estático

En la figura III.12 observamos cómo interconectar 3 redes mediante 2 *routers*.

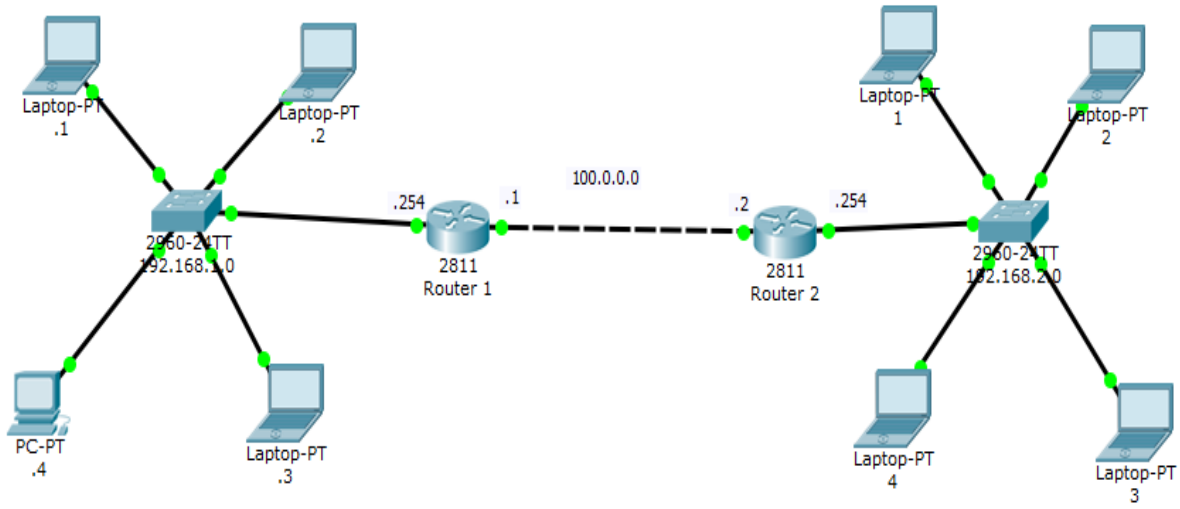


Fig. III.12. Topología física para interconectar 3 redes con 2 *routers*.

Una vez que se han hecho funcionales las LAN, las interfaces de los *routers* sólo existen en las tablas de enrutamiento de las redes contiguas. Por ejemplo, si intentamos enviar paquetes desde la LAN 192.168.1.0 a la 192.168.2.0, o viceversa, los paquetes se descartarán en el *router* 2 y 1, respectivamente, ya que ninguno de ellos cuenta en su tabla de enrutamiento con la tercera red, como se muestra en la figura III.13 para el *router* 1. Como ejercicio, el lector debe obtener la tabla de enrutamiento para el *router* 2.

```
Router1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
Router1#
```

Fig. III.13 Tabla de ruteo para el *router* 1 sin enrutamiento estático

¿Cómo se resuelve la conectividad?

Ahora es cuando entra en acción un administrador de red para realizar el enrutamiento estático, configurando manualmente –por ejemplo, en el *router* 2– lo necesario para agregar la red deseada, mediante la orden ***ip route***; entonces, se agrega la red, su máscara de subred y la interfaz a la que se debe dirigir en un *router* siguiente. La manera de configurar es la siguinte:

Router (config) #ip route 192.168.1.0 255.255.255.0 ***100.0.0.2***

Entonces, la tabla de enrutamiento queda como se indica en la figura III.14. Obsérvese que, además de las redes contiguas con la letra “C”, se indica la estática con la letra “S”.

```
Router2#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 100.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
Router2#
```

Fig. III.14 Tabla de ruteo para el *router* 2, ya con enrutamiento estático.

De esta manera, una vez que se configuran ambos *routers* y se verifica la conectividad entre los *hosts* de una red, al solicitarle al *router* sus tablas ARP y de enrutamiento se obtiene la figura III.15 para el *router* 1. Observe detalladamente los componentes y encabezados de cada una de las tablas. La figura III.16 muestra las tablas ARP y de enrutamiento para el *router* 2.

```
Router1#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  100.0.0.1              -   000D.BDC6.4A02  ARPA   FastEthernet0/1
Internet  100.0.0.2              7   0060.5CC8.8002  ARPA   FastEthernet0/1
Internet  192.168.1.1            7   00E0.F984.69EB  ARPA   FastEthernet0/0
Internet  192.168.1.2            7   00E0.B0BA.C419  ARPA   FastEthernet0/0
Internet  192.168.1.3            7   0060.47DC.22DB  ARPA   FastEthernet0/0
Internet  192.168.1.4            7   0003.E43D.B24C  ARPA   FastEthernet0/0
Internet  192.168.1.254          -   000D.BDC6.4A01  ARPA   FastEthernet0/0
Router1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 100.0.0.2
Router1#
```

Fig. III.15 Tabla ARP y tabla de ruteo para el *Router* 1.

```
Router2#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  100.0.0.1               7   000D.BDC6.4A02  ARPA   FastEthernet0/1
Internet  100.0.0.2               -   0060.5CC8.8002  ARPA   FastEthernet0/1
Internet  192.168.2.1             7   0040.0BD9.8403  ARPA   FastEthernet0/0
Internet  192.168.2.2             7   000C.8513.C2E9  ARPA   FastEthernet0/0
Internet  192.168.2.3             7   000B.BEC8.7B3B  ARPA   FastEthernet0/0
Internet  192.168.2.4             7   0001.9640.619A  ARPA   FastEthernet0/0
Internet  192.168.2.254           -   0060.5CC8.8001  ARPA   FastEthernet0/0
Router2#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 100.0.0.1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Fig. III.16 Tabla ARP y tabla de ruteo para el *Router* 2.

Con la finalidad de que el lector practique, realice, como ejercicio, la simulación correspondiente a la figura III.17. ¿Es posible comunicar a todas las redes? Explique.

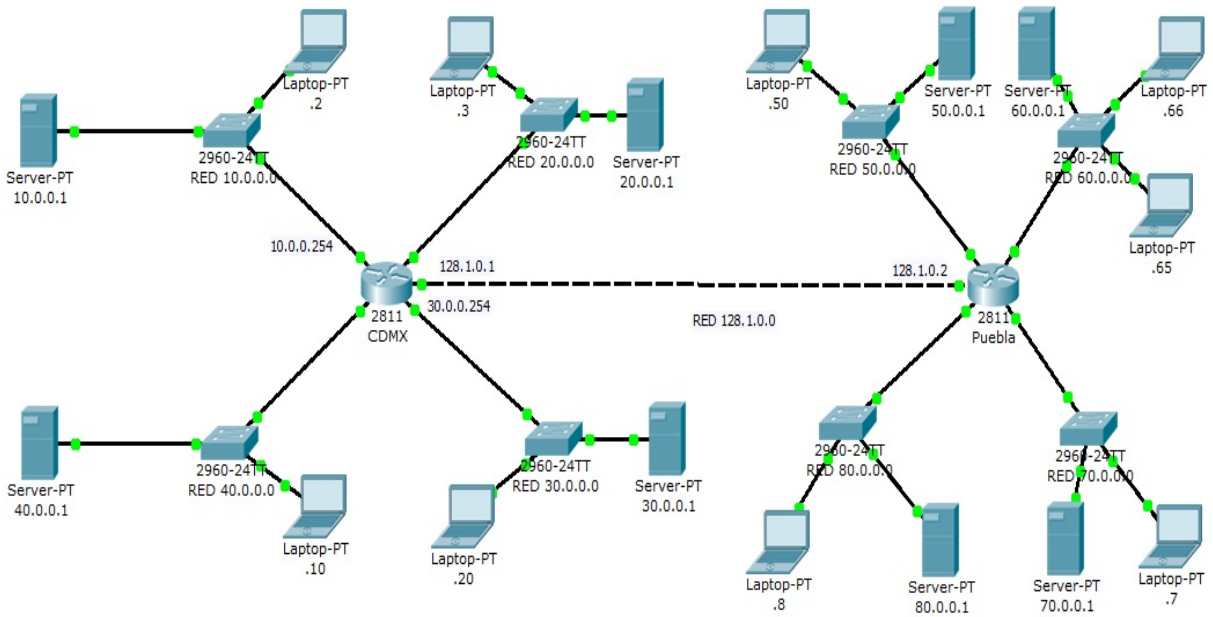


Fig. III.17 Topología física para interconectar 8 redes vía 2 *routers*.

Ahora veremos cómo se configura un circuito en el que se conectan 4 redes con 3 *routers*, para lo cual se emplea la topología de la figura III.18, que requiere el enrutamiento estático.

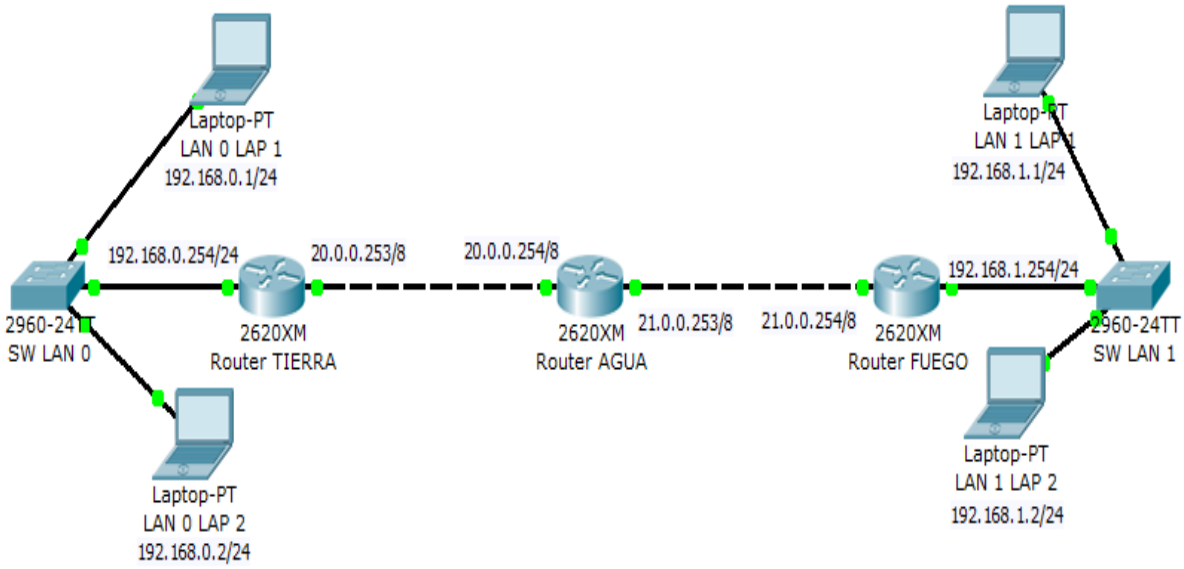


Fig. III.18 Topología física para interconectar 4 redes con 3 *routers*.

Una vez configurado y funcionando el circuito indicado, la tabla de enrutamiento para el *router* **Tierra** se observa como en la figura III.19, en la que se pueden apreciar a las 2 redes contiguas conectadas a las interfaces del *router*, más las 2 redes estáticas configuradas por un administrador, recordando que la tabla de enrutamiento se solicita con la orden: "*show ip route*". Mientras que la figura III.20 muestra la tabla ARP, la cual se solicita con la orden: "*show arp*". Analice cada una de las tablas a detalle.

```
C    20.0.0.0/8 is directly connected, FastEthernet0/0
S    21.0.0.0/8 [1/0] via 20.0.0.254
C    192.168.0.0/24 is directly connected, FastEthernet1/0
S    192.168.1.0/24 [1/0] via 20.0.0.254
```

Fig. III.19 Tabla de ruteo con 4 redes para el *router* **Tierra**.

```
TIERRA#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  20.0.0.253              -   000A.F3CD.DE45  ARPA   FastEthernet0/0
Internet  20.0.0.254             20   0090.0CDA.AEC1  ARPA   FastEthernet0/0
Internet  192.168.0.1            20   0001.C78D.42DA  ARPA   FastEthernet1/0
Internet  192.168.0.254           -   00E0.B08A.1601  ARPA   FastEthernet1/0
TIERRA#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  20.0.0.253              -   000A.F3CD.DE45  ARPA   FastEthernet0/0
Internet  20.0.0.254             23   0090.0CDA.AEC1  ARPA   FastEthernet0/0
Internet  192.168.0.1            23   0001.C78D.42DA  ARPA   FastEthernet1/0
Internet  192.168.0.254           -   00E0.B08A.1601  ARPA   FastEthernet1/0
```

Fig. III.20 Tabla ARP para el *router* **Tierra**.

Las figuras III.21 y III.22 muestran las tablas de ruteo y ARP para el *router* **Agua**.

```
C    20.0.0.0/8 is directly connected, FastEthernet0/0
C    21.0.0.0/8 is directly connected, FastEthernet1/0
S    192.168.0.0/24 [1/0] via 20.0.0.253
S    192.168.1.0/24 [1/0] via 21.0.0.254
```

Fig. III.21 Tabla de ruteo con 4 redes para el *router* **Agua**.

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	20.0.0.253	23	000A.F3CD.DE45	ARPA	FastEthernet0/0
Internet	20.0.0.254	-	0090.0CDA.AEC1	ARPA	FastEthernet0/0
Internet	21.0.0.253	-	0001.97D1.EE52	ARPA	FastEthernet1/0
Internet	21.0.0.254	17	00D0.FF96.7DB7	ARPA	FastEthernet1/0

Fig. III.22 Tabla ARP para el *router* **Agua**.

Finalmente, las figuras III.23 y III.24 muestran la tabla de ruteo y tabla ARP para el *router* **Fuego**.

```
S    20.0.0.0/8 [1/0] via 21.0.0.253
C    21.0.0.0/8 is directly connected, FastEthernet0/0
S    192.168.0.0/24 [1/0] via 21.0.0.253
C    192.168.1.0/24 is directly connected, FastEthernet1/0
```

Fig. III.23 Tabla de ruteo con 4 redes para el *router* **Fuego**.

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	21.0.0.253	17	0001.97D1.EE52	ARPA	FastEthernet0/0
Internet	21.0.0.254	-	00D0.FF96.7DB7	ARPA	FastEthernet0/0
Internet	192.168.1.2	12	0060.47DC.0A90	ARPA	FastEthernet1/0
Internet	192.168.1.254	-	0060.5C37.E449	ARPA	FastEthernet1/0

Fig. III.24 Tabla ARP para el *router* **Fuego**.

Como ejercicio, realice una simulación para agregar un *router* de nombre **Aire** al circuito de la red de la figura III.18, para obtener una topología de 5 redes con 4 *routers*.

III.6. Topología lógica e interconexión de redes MAN con *routers*

Dada la topología lógica de la figura III.25, observe la interconexión de las redes indicadas para la clase "C" y sus interfaces. Observe la redundancia e indique si existe cambio alguno en la red al desconectar los *routers* 1 y 5, y explique cómo afectan a la red esos cambios.

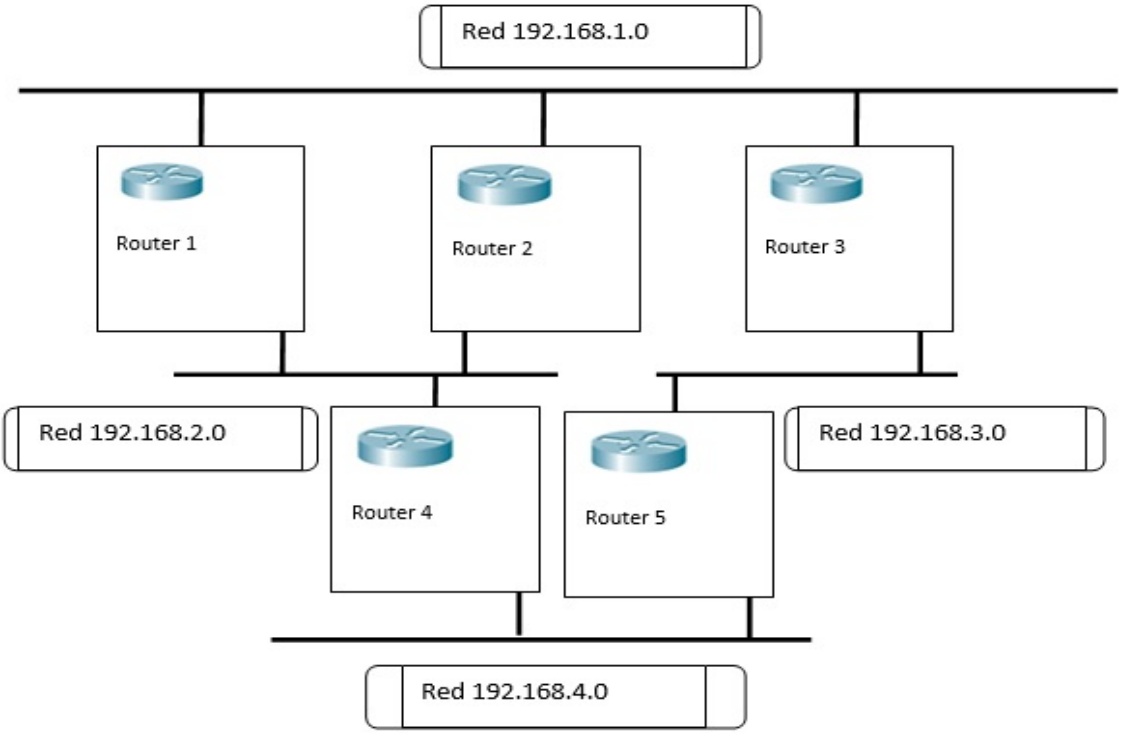


Fig. III.25 Topología lógica de N=4 redes interconectadas por N+1 *routers*.

III.7 PRÁCTICA 4: Enrutamiento estático

Actividad 1: Reproducir la simulación del circuito con las redes configuradas, con base en el enrutamiento estático indicado en la figura III.26. Pruebe la conectividad y obtenga las tablas ARP y de ruteo correspondientes, para cada uno de los 16 *routers,* comprobando todos los detalles de cada una de ellas.

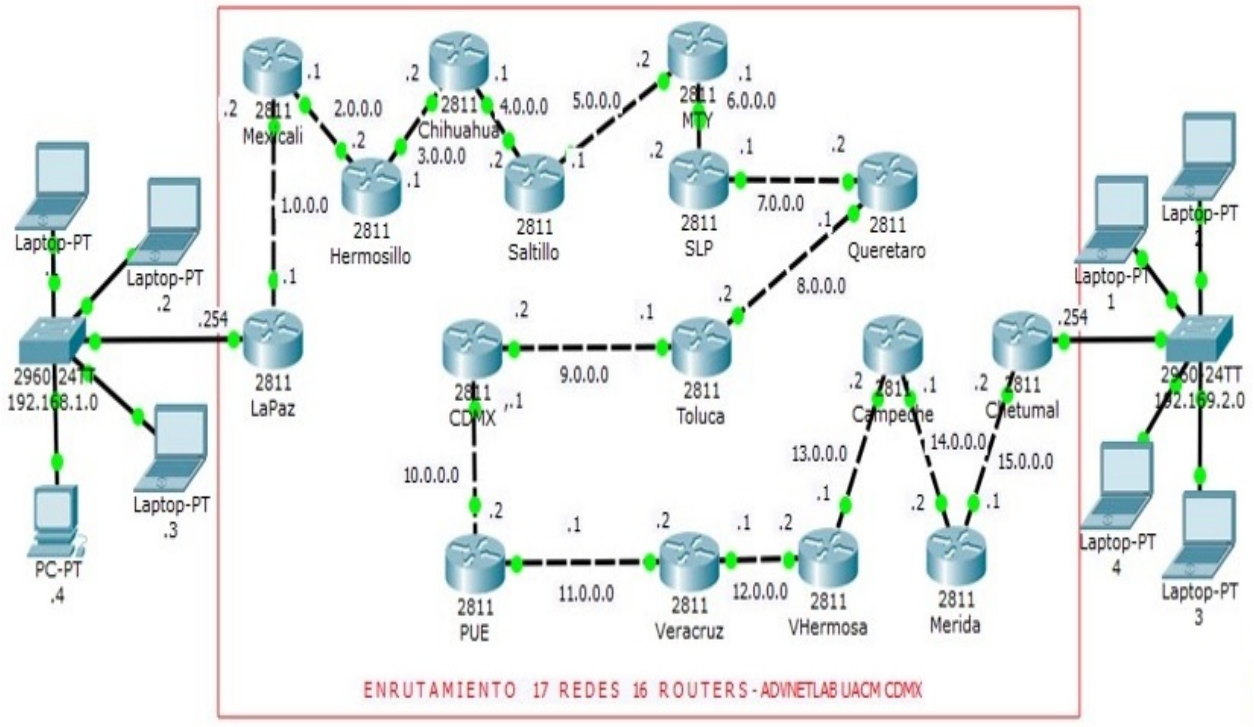


Fig. III.26 Topología física para 17 redes con 16 *routers*.

Actividad 2: De ser posible, practique el arranque y ordenes de monitoreo y configuración con un *router*. El *router* Cisco de la figura III.27 puede serle útil (e incluso podría comprar uno usado).

Fig. III.27 Router Cisco 7200 de *backbone*.

Actividad 3: Realice el análisis y la simulación del circuito de red de la figura III.28, de modo que use enrutamiento estático, y simúlelo para comprobar que existe conectividad entre cada *host*. Obtenga las tablas ARP y de enrutamiento.

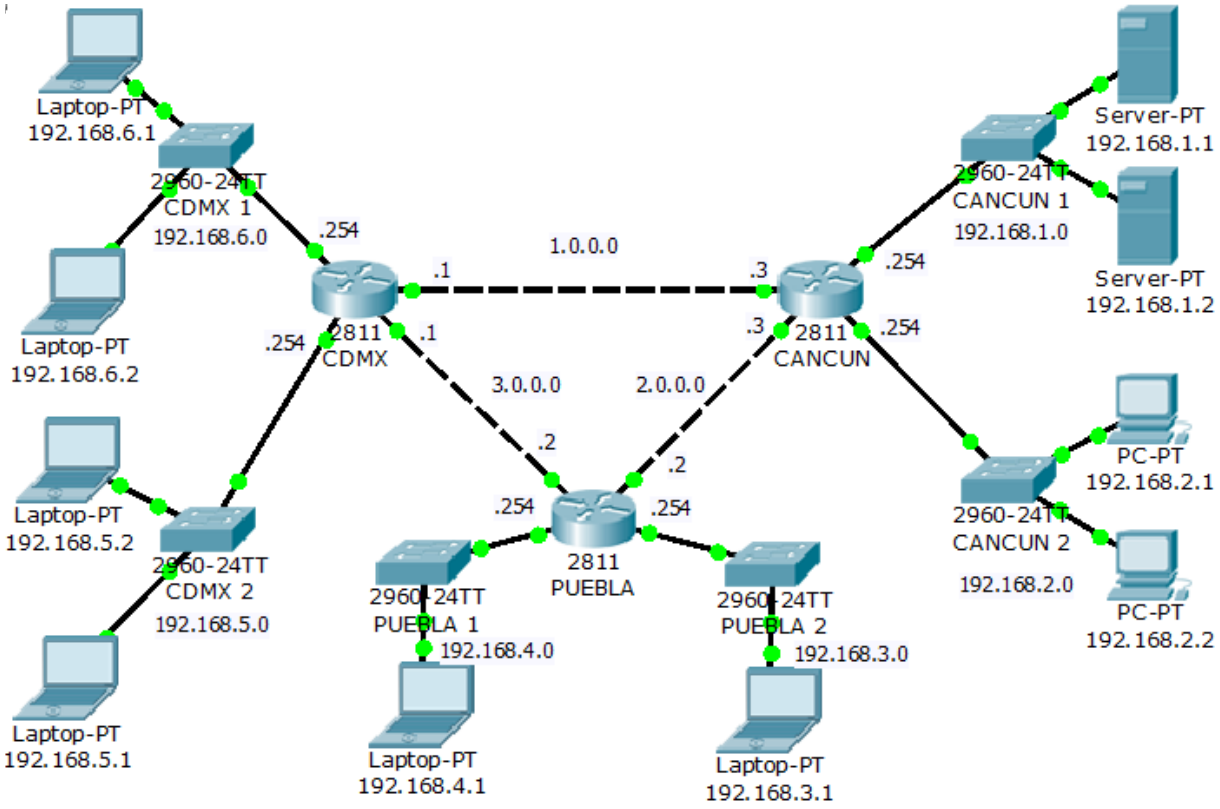


Fig. III.28. Ejercicio para enrutamiento estático.

III.8 Ethernet MAN Y WAN

Desde sus inicios, ARPANET pudo crear y conectar varias LAN y MAN, sin embargo, fue hasta 1988 que, con su sucesora, la red NSFNET, conformaría la primera red dorsal (***backbone***) WAN, la cual interconectaba sus 13 centros (entre ellos sus 6 centros de supercomputadoras), con las redes regionales y con ello conectaban a todo EUA. La NSFNET se conectó con ARPANET vía un IMP. En 1989 se usó fibra óptica para crear el segundo *backbone* a 488 kbps.

- **La comercialización de la red global**

En 1990 se apagó ARPANET, quedando el backbone de NSFNET, el cual se actualizó a 1.5 Mbps. Debido al crecimiento exponencial en el uso de esta infraestructura de red, el gobierno de EUA, al no darse abasto, la vendió a un consorcio de tres empresas: IBM, MCI y MERIT. Estas empresas actualizaron el backbone a 45 Mbps y, con ello, esta red se redefinió como *Advanced Network and Services* (ANSNET), permitiendo la interconexión entre redes regionales que ya abundaban, por lo que dio concesiones para crear un Punto de Acceso a la Red (*Network Access Point- NAP*), de modo que todo operador debía conectarse con los 4 NAP concesionados: Sprint-NY, MFS-WDC, Ameritech-Ch y Pacbell-SF. Entre 1992 y 2002, tanto Europa, como Asia y algunos países de Latinoamérica repitieron el modelo **[2]**.

En 1990, la tecnología Ethernet se encontraba muy madura en el ámbito LAN y había crecido exponencialmente en todo el mundo. El crecimiento en la demanda de aplicaciones de banda ancha, a costos cada vez menores, empujó a los proveedores de servicios de Internet para que buscaran cómo migrar sus sistemas de LAN a MAN; por lo que nació el MAN Ethernet o Metro Ethernet, que consiste en una MAN hecha con base en Ethernet. Rápidamente, Metro Ethernet se hizo muy popular, superando a las versiones de fibra óptica SONET/SDH o PDH en las redes de los ISP, de modo que los niveles de distribución o agregación se movieron hacia esta tecnología **[16]**. Conforme los proveedores iniciaron los servicios Metro Ethernet, se permitió que el estándar IEEE 802.1Q-2005 (VLAN *Bridges*) asignara, a cada instancia del servicio del cliente, su propio ID del VLAN, para garantizar la seguridad del tráfico y el uso óptimo del ancho de banda; pero ello limitó el número máximo de las instancias de servicio, que un proveedor podría ofrecer sobre una red, a 4094 VLAN permitidas. Por esta limitación, se desarrolló el estándar IEEE802.1ad-2005 *Provider Bridges* (PB), que estandariza la arquitectura y los protocolos de *bridging* para permitir que las tramas Ethernet tengan múltiples etiquetas VLAN. El estándar quedó dentro de la norma IEEE 802.1Q-2005. Si consideramos, por ejemplo, que un proveedor de servicios ofrece un servicio LAN transparente a una empresa con 50 *sites* y 200 *end systems* por

site, entonces, los *switches* del proveedor de servicio deben aprender 10,000 direcciones. Y, si el proveedor tuviese sólo 10 clientes, cada uno de ellos con esas características, entonces sus equipos deberían aprender 100,000 direcciones, lo cual excedía la capacidad de la mayoría de los *switches* disponibles en el mercado, ya que, en ese tiempo, tenían entre 4,000 a 64,0000 registros para direcciones MAC. De modo que, al menos, había dos problemas: las instancias de los servicios y las limitaciones de escalabilidad de las direcciones MAC. Lo anterior motivó el desarrollo del estándar IEEE 802.1Qah-2008, el *Provider Backbone Bridges* (PBB), el cual define protocolos *bridge* y una arquitectura de interconexión de redes de *bridge* para el proveedor (PBN). La trama Ethernet incluye las direcciones MAC Backbone fuente y destino. El PBB extiende a la versión **ad** de la norma señalada, al introducir un modelo de arquitectura de red jerárquica que habilita a los proveedores de servicios para construir redes *bridged* grandes. En este modelo, las redes *bridges* 802.1Q se agregan dentro de redes de *bridge* de proveedor 802.1ad, las cuales, a su vez, se añaden dentro de una red de *bridges* de *backbone* de proveedor.

Para resolver el problema de la escalabilidad de las direcciones MAC, PBB introdujo un nuevo formato de trama que provee un esquema de "encapsulamiento" del "tunelamiento" MAC, en el cual: las tramas del cliente se encapsulan en las tramas Ethernet del proveedor, conforme ingresan a la red PBB, por lo que se esconde la dirección del cliente al PBB núcleo o *core*. Los equipos en el núcleo de una red PBB, reenvían el tráfico, con base en la dirección MAC *backbone* (B-MAC), lo cual confina el requerimiento de aprender la dirección del cliente en los equipos de la orilla de la red PBB. Tales equipos (*edge devices*) se llaman *Backbone Edge Bridges* (BEB). Un BEB determinado, sólo debe aprender las direcciones de los clientes a los que les da soporte y sólo se requiere que un equipo de núcleo aprenda las direcciones del BEB, en lugar de tener que aprenderse todas las direcciones de todos los equipos de cliente final (*end customer device*). Los 3 aspectos anteriores, relacionados con la escalabilidad, quedaron dentro del estándar IEEE 802.1Q-2011 **[16]**.

Posteriormente, se continuó con la lógica de llevar Ethernet a WAN, incluso a nivel de *backbone,* para hacerlos más afines a Ethernet. Así nació el llamado *Ethernet Carrier,* portador de Ethernet, o portador de backbone. Para 2008, Ethernet ya estaba posicionado como una tecnología de acceso para los proveedores de servicios y redes portadoras de la siguiente generación, en la que las redes núcleo (*Core networks*) de los proveedores de servicios, en los que convergen las tecnologías IP y *Multi-Protocol Label Switching* (MPLS), y muchos de los *routers* tipo *core* ya podían albergar, en sus tablas de enrutamiento, hasta 1 millón de rutas **[16-17]**. Para profundizar

en el tema de Ethernet MAN y WAN, se deja al interés de los lectores que se vayan relacionando con el *backbone* de los ISP en su carrera laboral.

III.9 *Router, modem, switch y firewall* casero, ofrecido por un ISP

Cuando un cliente contrata un servicio para casa habitación, su ISP le proporciona el equivalente a una roseta en telefonía convencional y un equipo, el cual es un *modem, router, switch, firewall y access point* (MRSFA), al que convencionalmente la gente llama simplemente *modem*. Si cuenta con *login* y *password,* acceda al equipo para revisar su configuración o cambiarla en su caso, como se indica en la figura III.29.

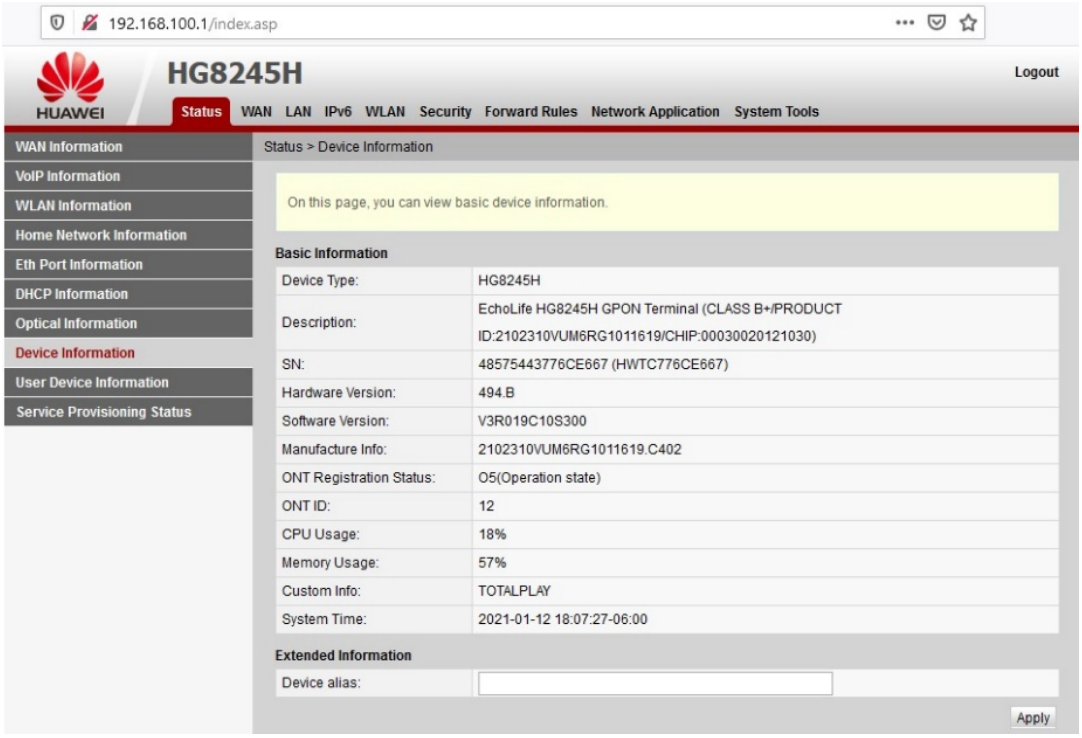


Fig. III.29. Interfaz gráfica al acceder al *gateway* de la LAN.

Cuando se trata de una interfaz de fibra óptica del ISP y el cableado del usuario, a la roseta o caja donde se interconectan el MRSFA y el ISP se le llama terminal óptica de red (*Optical Network Terminal* - ONT). En el caso de la figura III.29, observe cómo se indica que el equipo se encuentra en estado operacional, así como el uso de CPU y RAM del MRSFA.

La figura III.30 muestra información acerca de la conectividad óptica, mostrando una potencia de recepción de -23 dBm. Observe también los valores de voltaje y corriente.

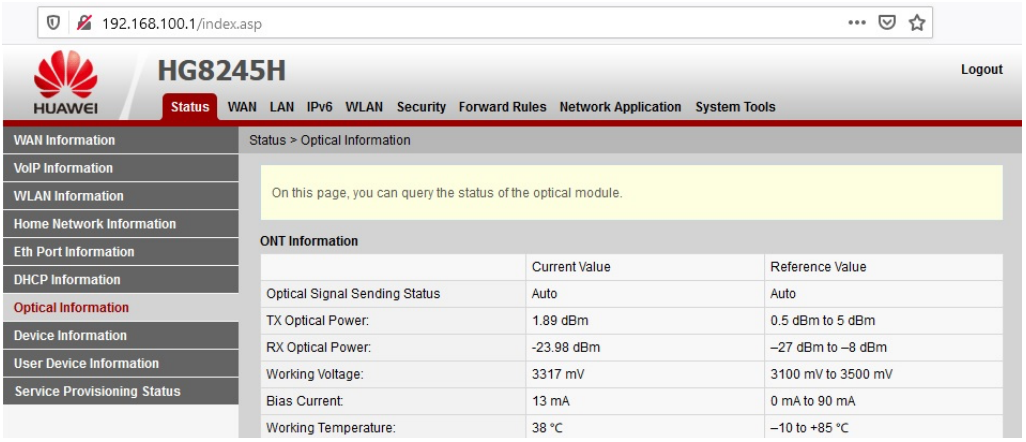
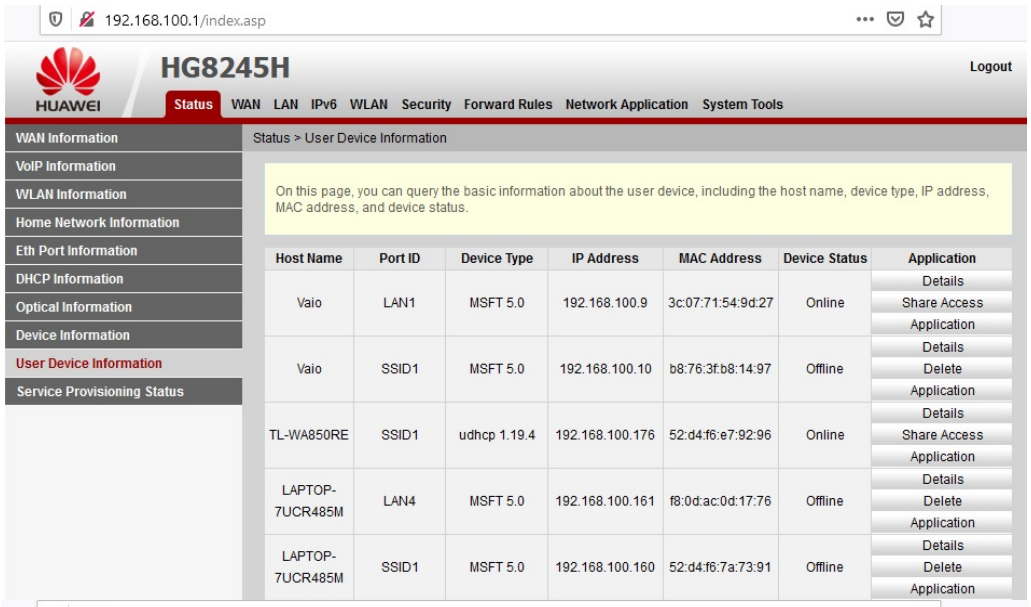


Fig. III.30. Características y valores para la interfaz óptica que llega desde el ISP.

Mientras que, en la figura III.31ª, se puede observar el equivalente a la tabla ARP del *router*, con las direcciones lógicas y físicas, así como las interfaces. En la III.31B se observa exclusivamente el estado de las 4 interfaces Ethernet.

(A)



(B)

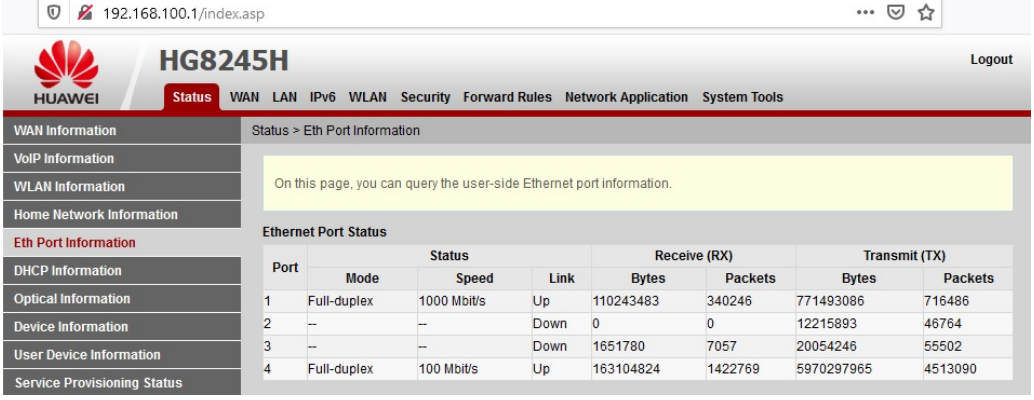


Fig. III.31. A) Equivalente a tabla ARP del *router*. B) Información sólo para las 4 interfaces Ethernet

Si nos preguntamos ¿cuántos equipos hay conectados en la LAN y a cuáles el DHCP les ha brindado alguna dirección IP? Tenemos un total de 11 hosts en la red 192.168.100.0, asignados por DHCP, asignados por DHCP como puede comprobarse con la figura III.32

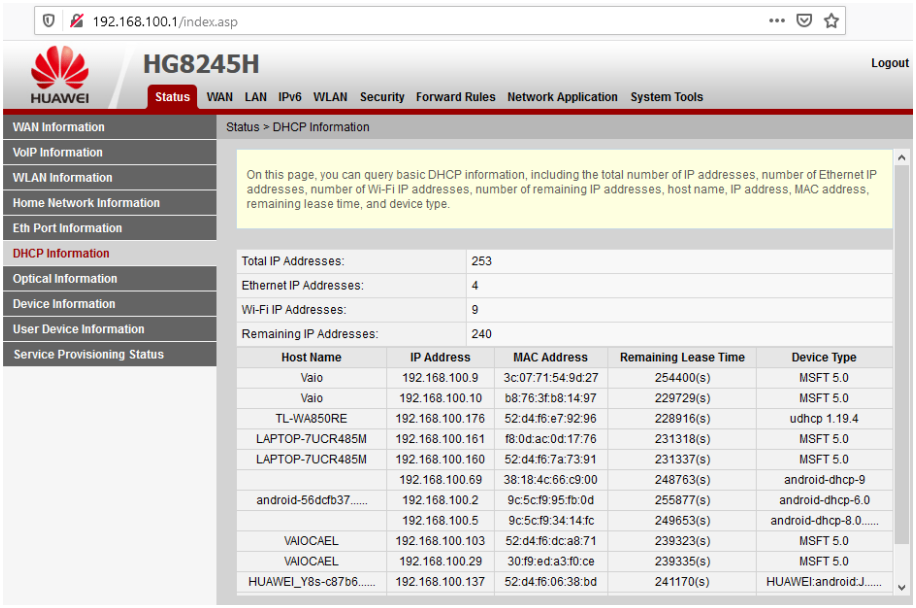


Fig. III.32. Equipos conectados en la LAN.

Si se desean observar los detalles de la seguridad, la autentificación y encriptación, éstos se presentan en la figura III.33. El servicio del ISP muestra 75 Mbps para bajada y 8 Mbps para subida, con una latencia de 4 ms, al enviar un ping de reconocimiento.

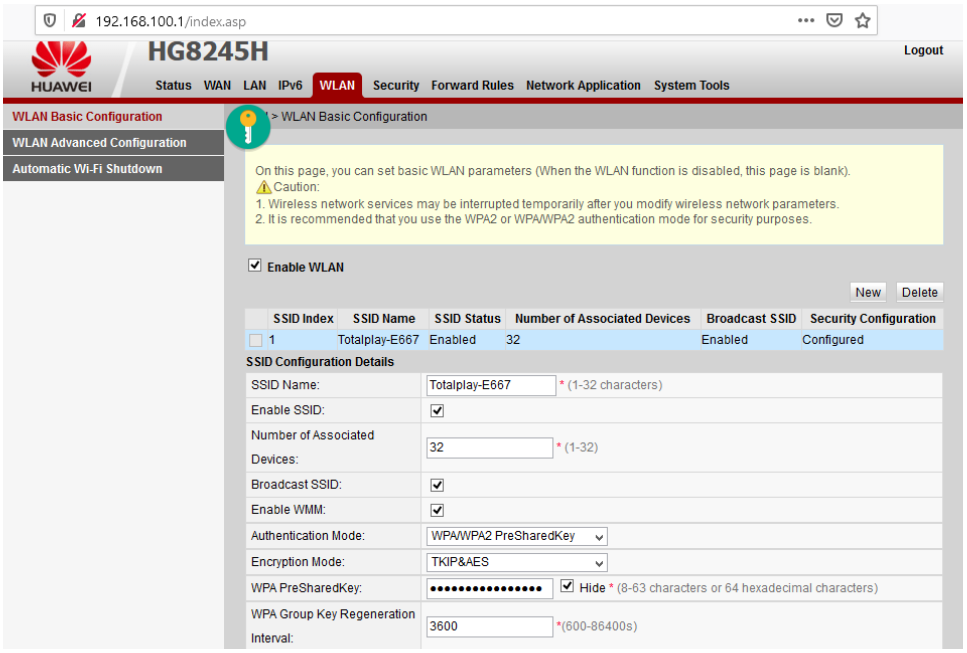


Fig. III.33. Modos de autentificación y encriptación.

CAPÍTULO IV: ENRUTAMIENTO DINÁMICO

Una vez que las redes crecían, en tamaño y complejidad, se buscó implementar una búsqueda de *routers* vecinos y rutas que llevaran paquetes desde un origen hacia un destino en otras redes; para ello se revisaron los algoritmos que resolvían le problema del viajero, para encontrar rutas óptimas. Los algoritmos dieron lugar a protocolos y estos se pudieron clasificar en aquellos de enrutamiento interior, para los equipos que administraba un mismo ISP, o de enrutamiento exterior, para interconectarse con equipos que administraba otro ISP.

IV.1 Protocolos de enrutamiento

Desde los inicios de ARPANET, con la finalidad de interconectar redes se emplearon los IMP y éstos evolucionaron a *gateways*. Conforme la red continuaba creciendo, fue necesario interconectar varios *gateways*, para ello se emplearon **protocolos de enrutamiento** conocidos como protocolos de *gateway*. A medida que ARPANET y NSFNET se expandieron, los *gateways* dejaron su lugar a los *routers* y éstos se fueron agrupando en distintos niveles de infraestructura; de modo que se contó con *routers* para el acceso, los del nivel de distribución y el nivel de núcleo (*backbone*). En su evolución y transición, un conjunto de *gateways o routers* de *backbone,* manejado por un ISP, fue definido como sistema autónomo (*Autonomous Systems* - AS). Los *gateways* requerían de protocolos que permitieran un óptimo desempeño al interior de los AS –éstos se conocen como *Interior Gateway Protocol* (IGP) –. Mientras que para manejar grupos de AS – que pertenecieran a un mismo ISP o a distintos ISP –, se crearon los *Exterior Gateway Protocol* (EGP). Finalmente, para interconectar a los AS, se generaron los *Border Gateway Protocol* (BGP). En la figura IV.1 se muestra una clasificación de los protocolos de enrutamiento. En este capítulo se abordarán los protocolos RIP y OSPF.

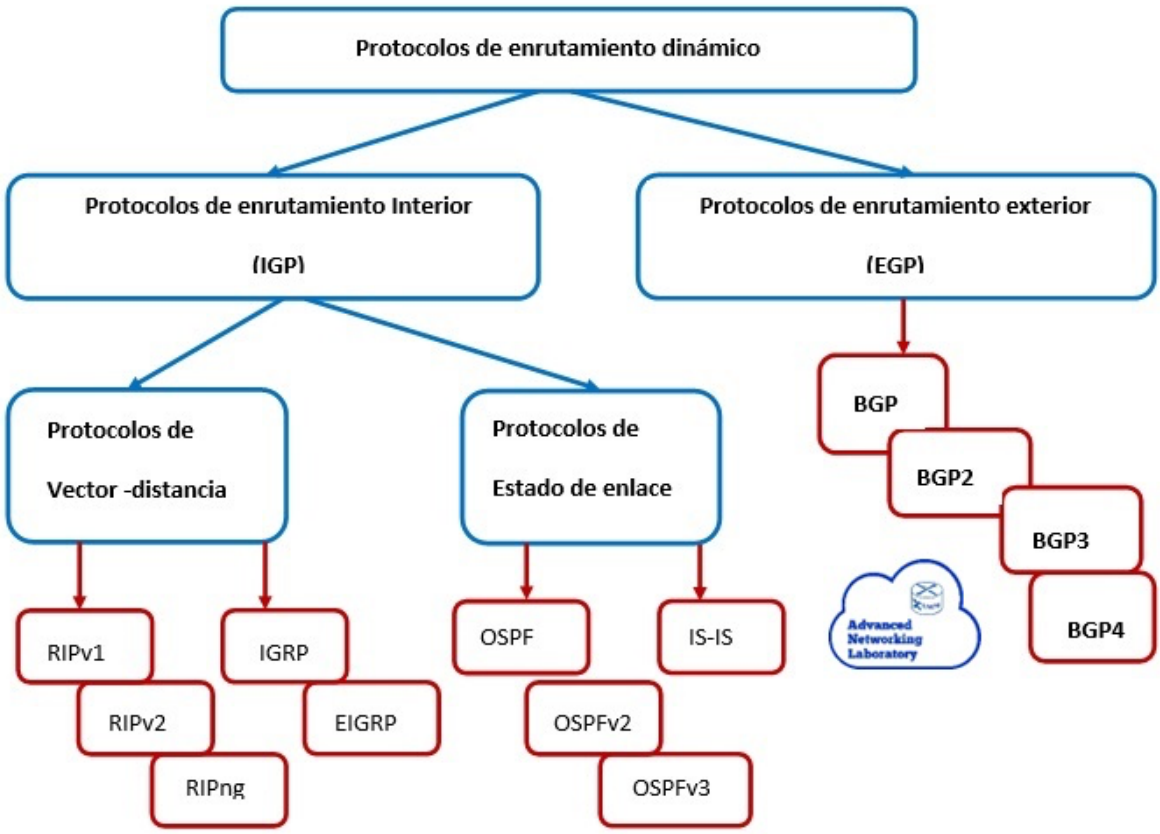


Fig. IV.1. Clasificación general de los protocolos de enrutamiento dinámico.

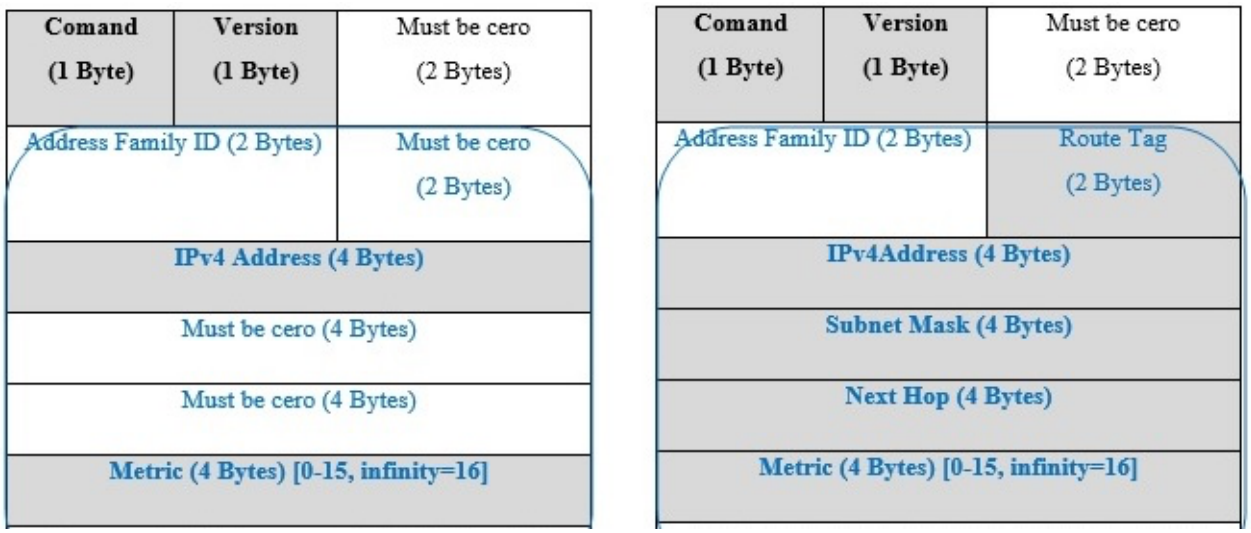
IV.2 RIP

El primero de los protocolos de enrutamiento IGP estandarizados fue el *Routing Information Protocol* (RIP), el cual emplea el algoritmo Bellman-Ford, y podemos encontrar las versiones e RIPv1, en el RFC 1058 de 1988; RIPv2 en el RFC 1388 de 1993; RIPv2 en el RFC 1723 de 1994; RIPv2, en el RFC 2453 de 1998; RIPv2, en el RFC 4822 de 2007; todas esas son versiones para IPv4 **[18-22]**. Mientras que el RFC 2080, de 1997, es la versión de RIP para IPv6 **[23]**.

El funcionamiento del RIP se fundamenta en el algoritmo Bellman-Ford, el cual es del tipo vector distancia y es una evolución de la función "*routed*" incluida en Unix BSD de 1982. RIP hace que los mensajes de actualización, que tienen información para el llenado de las tablas de enrutamiento, estén en los paquetes RIP, los cuales viajan en la capa L3, en ellos están encapsulados los datagramas del tipo UDP y, para esto, se usa el puerto 520. La métrica que usa RIP son los saltos y una red debe tener un máximo de 15 saltos, pues se considera inalcanzable una red que requiere 16 saltos o más.

Un paquete RIP se compone de 2 partes: el encabezado RIP, de 4 bytes, y un máximo de 25 entradas de ruta, de 20 bytes por cada una de las rutas. Es decir, un paquete RIP que contenga el mínimo de una ruta medirá 24 bytes, pero si contiene las 25 rutas tendrá como un máximo 504 bytes. RIP tiene varios relojes (*timers*) o temporizadores, los cuales utiliza para preguntar a sus vecinos acerca de nuevas rutas y así poder añadirlas a su tabla de enrutamiento. Para la actualización de las rutas, el protocolo lo realiza cada 30 segundos; mientras que para invalidar una ruta usa un temporizador que espera 180 segundos. Si alguna ruta no se actualiza, será eliminada de la tabla de enrutamiento.

La figura IV.2 muestra los formatos de los paquetes RIPv1 y RIPv2. Obsérvese que los primeros 4 Bytes corresponden a la cabecera, mientras que cada "entrada" de la red tiene 20 bytes. RIP tiene una capacidad máxima de 25 "entradas", para 25 redes, de manera simultánea.



A B

Fig. IV.2. A) Formato de paquete RIPv1. B) Formato de paquete RIPv2

IV.2.1 Evolución de RIP

En la tabla IV.1 se muestra la evolución de los RFC para RIP en sus diferentes versiones.

Proposed Standard	Draft Standard	Internet Standard	Historic
RIP v1			
→	→	→	**RFC 1058-1988**
RIP v2			
RFC 1388-1993		RFC 1723-1994	
		RFC 2453-1998	
RFC 4822-2007 Cryptographic authentication			

Tabla IV.1 Evolución del estándar RIP.

Características de RIPv2

a) Mantuvo los 15 saltos máximos (16 inalcanzable) como única métrica, de modo que su tiempo de convergencia no es muy corto.

b) Permitió subredes: CIDR y VLSM.

c) Autentificación usando MD5, por ello usa la primera de las 25 entradas y deja sólo 24 para las entradas de las redes. La mejora criptográfica se propuso en 2007, pero no prosperó.

d) En lugar de mantener el puerto 520 vía broadcast a la dirección 255.255.255.255, usa la dirección *multicast* 224.0.0.9 (Clase D).

IV.3. Redes con RIPv1

Si consideramos el circuito de la figura IV.3 y revisamos sus tablas ARP y de enrutamiento, como en la figura IV.4, observamos que no es posible la comunicación entre las redes 192.168.1.0 y la 10.0.0.0 sin que se le indique a cada *router* que las redes existen.

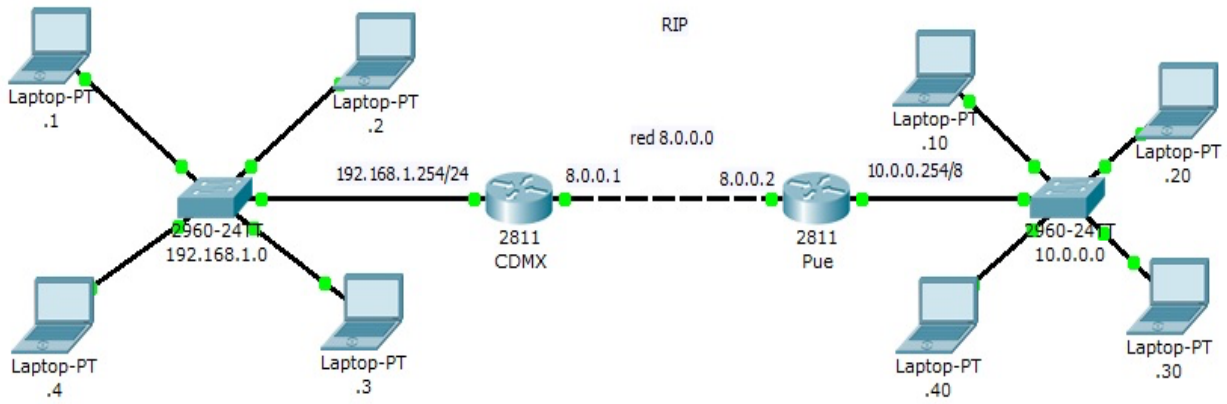


Fig. IV.3. A) Formato de paquete RIPv1. B) Formato de paquete RIPv2

```
CDMX#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  8.0.0.1                   -   0060.3E42.7502  ARPA   FastEthernet0/1
Internet  192.168.1.1               2   0090.2199.0D4A  ARPA   FastEthernet0/0
Internet  192.168.1.254             -   0060.3E42.7501  ARPA   FastEthernet0/0
CDMX#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    8.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Fig. IV.4. Tablas ARP y de enrutamiento, sin enrutamiento estático o dinámico.

En esta ocasión no se hará de manera estática, sino que en cada router se habilitará el uso del protocolo RIP, configurándolo en cada una de sus interfaces, como se indica en la figura IV.5, y el protocolo se encarga del resto, siguiendo un proceso que veremos a detalle. La misma configuración RIP se ejecuta en el *router* "Pue", de modo que ambos *routers* pueden "hablar" el mismo idioma a través de sus interfaces que los conectan mediante la red 8.0.0.0.

```
CDMX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CDMX(config)#router rip
CDMX(config-router)#network 8.0.0.0
CDMX(config-router)#exit
CDMX(config)#exit
CDMX#
```

Fig. IV.5. Configuración RIP en *router* CDMX.

Sin embargo, si en este momento solicitamos la tabla de enrutamiento, ésta seguirá como se observa en la figura IV.4, ya que para que se dé de alta la nueva red, se debe completar el proceso, el cual revisamos a continuación. La figura IV.6 muestra un paquete que se genera desde L5 y se encapsula en L4, como un datagrama que se usa el puerto 520, y éste se empaqueta en L3 usando una dirección destino de broadcast (255.255.255.255), desde la interfaz indicada como 8.0.0.2, ubicada en el *router* Pue y se dirigirá hacia el *router* CDMX.

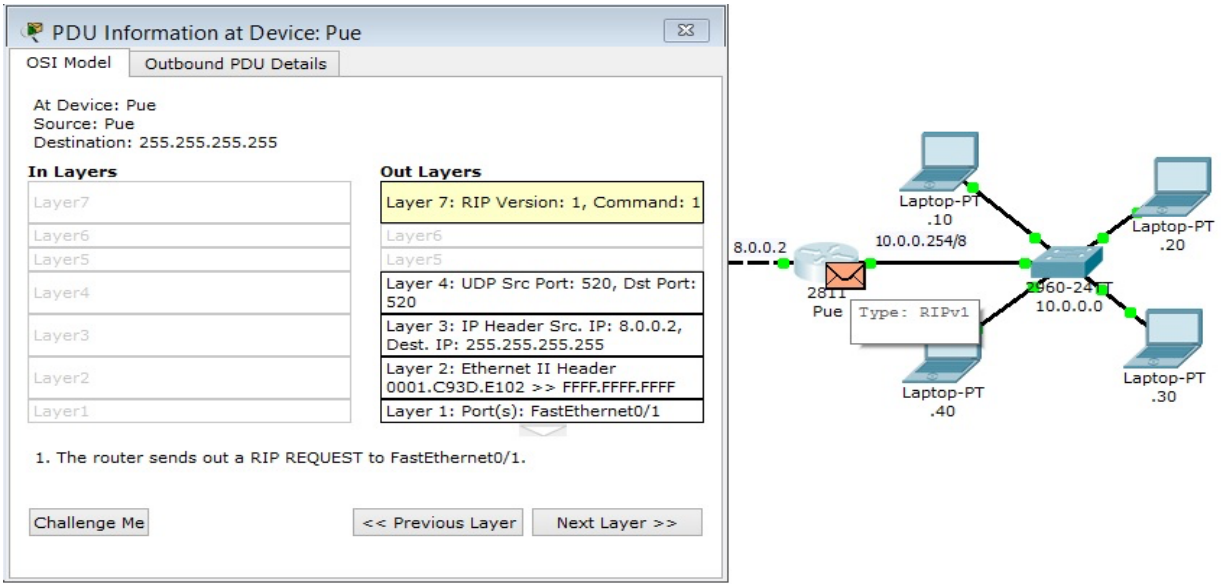


Fig. IV.6. Paquete RIP v1 desde el *router* Pue, hacia el *router* CDMX, y su mapeo en TCP/IP.

La figura IV.7 muestra los detalles del paquete RIPv1 en L3 y del datagrama UDP en L4, los cuales están encapsulados en la trama en L2. En este punto podemos comparar el formato del paquete RIPv1, de la figura IV.2A, el cual viene del RFC, mientras que la figura IV.7, muestra los detalles del paquete de acuerdo con el simulador Cisco *Packet Tracer*. Note que los primeros 4 bytes pertenecen al encabezado. Observe también que, en IV.7, erróneamente se indica "*Next Hop*", ya que los programadores, de alguna manera, han considerado la adecuación al RIP v2, sin

embargo, queda vacío al respetar el protocolo RIPv1. Estos detalles aparecerán, o no, en función de la versión del simulador Cisco *Packet Tracer* que el lector use. Además, siempre es posible detectar algunos "bugs".

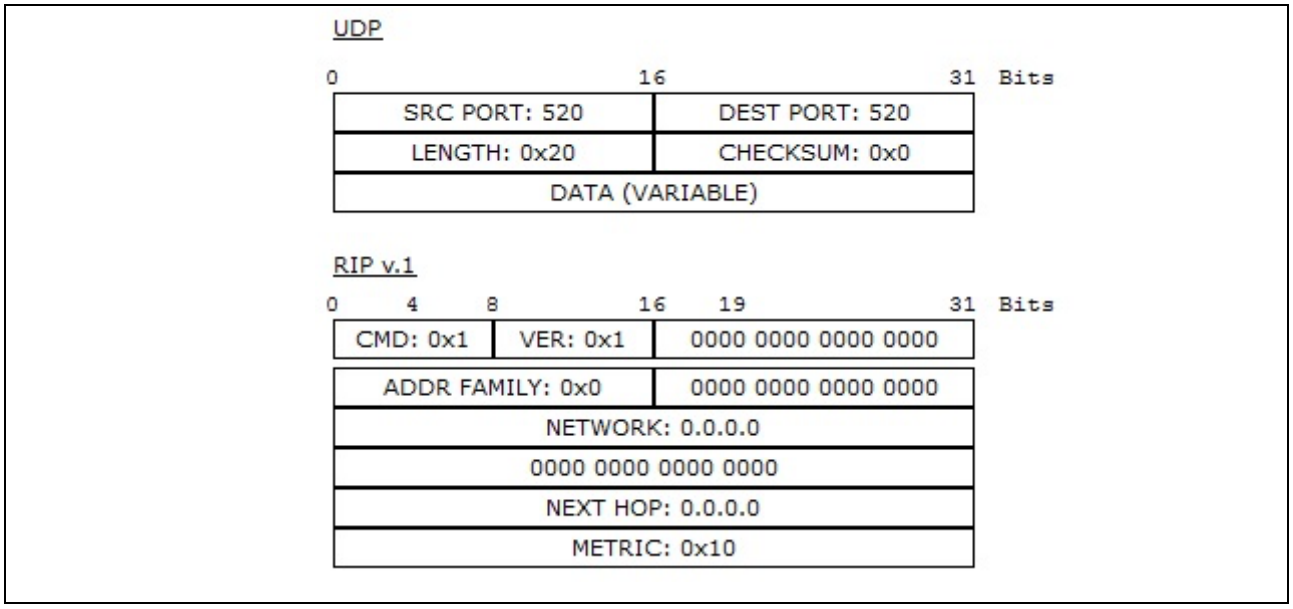


Fig. IV.7. Paquete RIP v1 desde el *router* Pue hacia el *router* CDMX y su mapeo en TCP/IP.

Lo que se recomienda, a la hora de configurar cualquier protocolo, es que se habilite en todas las interfaces que un *router* tiene activas, para que los paquetes se propaguen por todas sus interfaces, compartiendo el contenido de sus tablas de enrutamiento y descubriendo, de esta manera, las redes nuevas para cada *router*. Una vez configuradas ambas interfaces en los *router,* los paquetes RIPv1 se preparan para propagarse en la red, como se muestra en la figura IV.8.

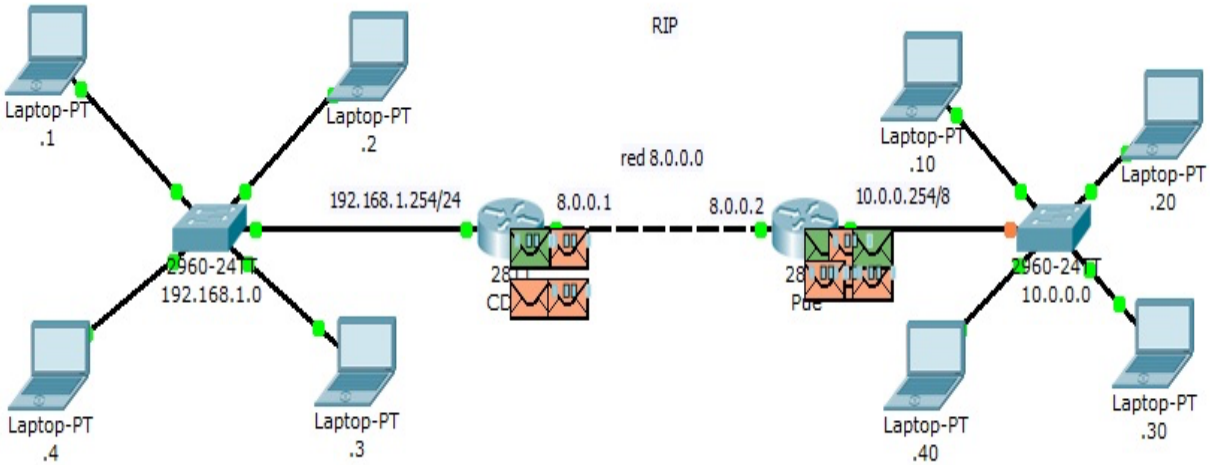


Fig. IV.8. Paquete RIP v1 desde el *router* Pue hacia el *router* CDMX y su mapeo en TCP/IP.

También debe observarse que, cuando los paquetes RIPv1 se propagan, cada *router* recibe el paquete, lo desencapsula e "interpreta"; sin embargo, una vez que cada *switch* reenvía a los *hosts* los paquetes RIPv1, entonces cada *host* recibe los bits como tramas. El desencapsulamiento extrae los paquetes para interpretarlos, en la capa L3, y la instrucción es desencapsularlos para recibirlos en la L4, pero a la hora de identificarlos, los *hosts* no reconocen al servicio RIP, de modo que desechan esos paquetes, como se indica en la figura IV.9.

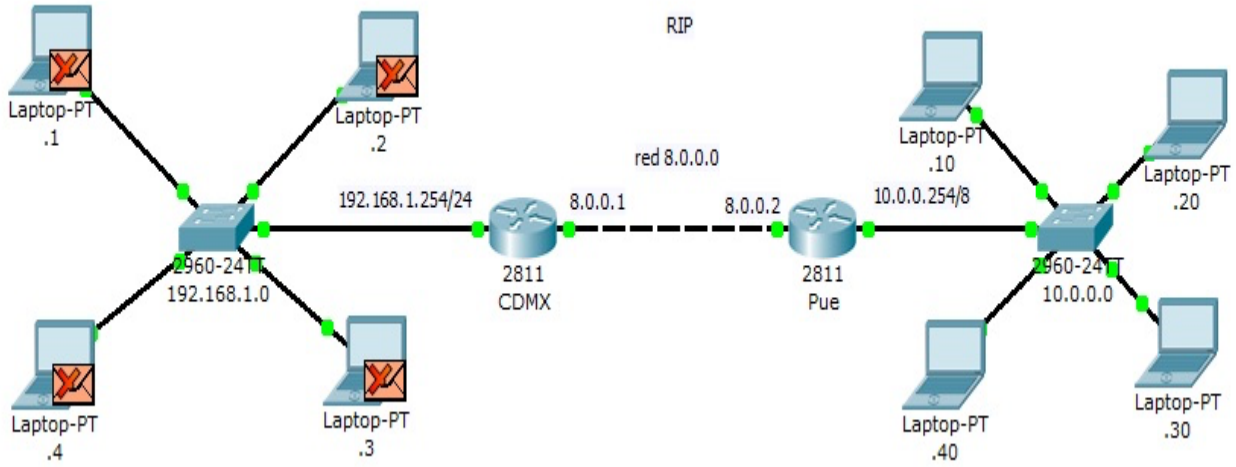


Fig. IV.9. Paquetes RIP v1 que llegan a los *hosts* y que son desechados en la L4.

Sin embargo, los paquetes que llegan, desde un *router* a otro, llevan los paquetes RIPv1, como se indica en la figura IV.10. Aquí debe observarse que el paquete RIPv1 cuenta con 2 entradas: en una de ellas se indica la existencia de la red 8.0.0.0 y en la red 10.0.0.0., y para cada caso se muestra el número de saltos en los que se encuentran. Observamos que para la red 10.0.0.0 se señala la métrica 2 porque este paquete fue uno de los que llegó al *host* y fue desechado; pero si hubiese llegado a otro *router*, estaría señalando que para llegar a la red 8.0.0.0 debe dar 1 salto y que para llegar a la red 10.0.0.0 debe dar 2 saltos.

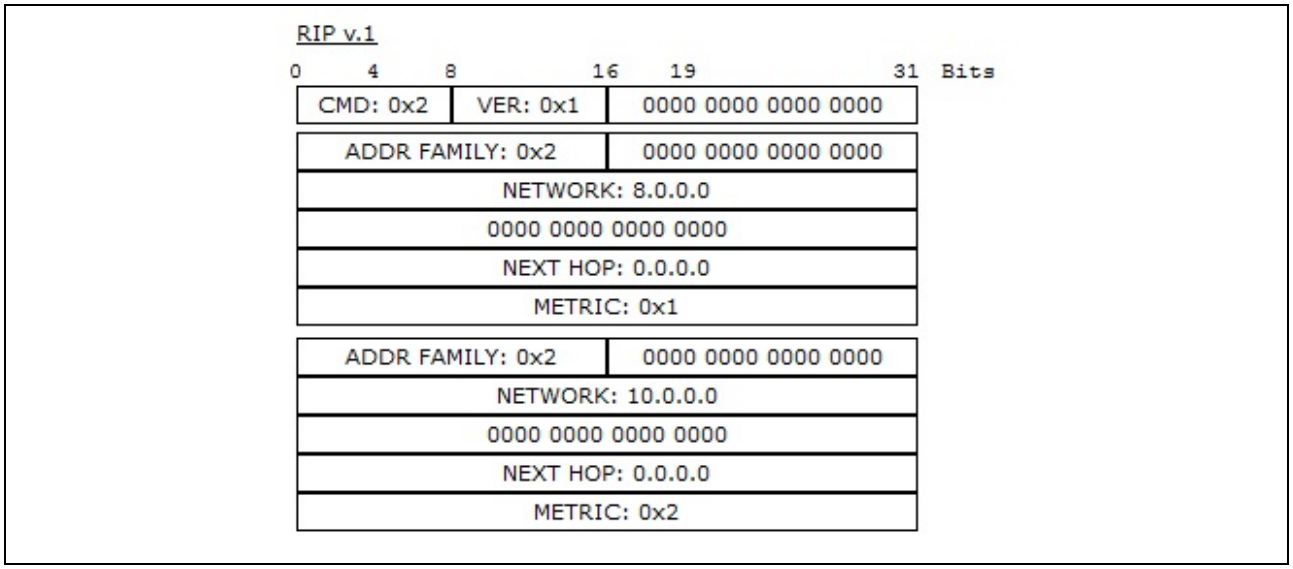


Fig. IV.10. Paquete RIP v1 desde el *router* Pue, hacia el *router* CDMX, y su mapeo en TCP/IP.

Una vez que los paquetes RIPv1 llegan a los *routers*, éstos actualizan sus tablas de enrutamiento, como se hace evidente en la figura IV.11 del *router* CDMX, y lo mismo sucede con el *router* Pue.

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

Gateway of last resort is not set

C    8.0.0.0/8 is directly connected, FastEthernet0/1
R    10.0.0.0/8 [120/1] via 8.0.0.2, 00:00:00, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
CDMX#
```

Fig. IV.11. Tabla de enrutamiento para el *router* CDMX.

En cada tabla de enrutamiento se observa, además de las 2 redes contiguas ya conocidas, la nueva red, indicada con una **R**, la cual fue agregada gracias al protocolo RIP. La figura IV.12 muestra la tabla de enrutamiento para el *router* Pue. Obsérvese entonces que, una vez terminado el proceso de llenado de tablas cada 30 segundos, cada *router* envía paquetes RIPv1 a través de sus interfaces, para que, de existir nuevas redes, las tablas se vayan actualizando.

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

Gateway of last resort is not set

C    8.0.0.0/8 is directly connected, FastEthernet0/1
C    10.0.0.0/8 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 8.0.0.1, 00:00:25, FastEthernet0/1
Pue#
```

Fig. IV.12. Tabla de enrutamiento para el *router* Pue.

De manera adicional, para obtener la configuración de aquello que se está ejecutando en cada *router,* usamos la orden "sh run", de modo que observamos que al menos en la RAM está indicada la configuración del protocolo RIPv1, como se indica en la figura IV.13

```
interface FastEthernet0/0
 ip address 10.0.0.254 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 8.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 network 8.0.0.0
 network 10.0.0.0
!
ip classless
!
```

Fig. IV.13. Tabla de enrutamiento para el *router* Pue.

Pero ¿qué sucede con aquellas redes que se van retirando de la red? Éstas se marcan con una bandera, gracias a un contador o temporizador; un segundo temporizador arranca a los 120 segundos, el *timer* "*garbage collection*" y, finalmente, cuando no existe actualización de su

presencia por un total de 180 segundos, entonces se borran de las entradas de las tablas de enrutamiento. De este modo, en una red, todos los *routers* tendrán conocimiento acerca de todas las redes, permitiendo así una conectividad total.

En este punto, es posible probar la conectividad vía PDU en el simulador o vía ping. Como ejercicio, resuelva la topología de la red de la figura III.17 (Topología física para interconectar 4 redes con 3 *routers*.), pero con RIPv1, para obtener las correspondientes tablas ARP y de enrutamiento.

IV.4 Redes con RIPv2

Si consideramos la red de la figura IV.3, pero ahora deseamos que entre en funcionamiento el protocolo RIPv2, en lugar del protocolo RIPv1, se opta por la secuencia indicada en la figura IV.14A, en la que se agrega versión 2; mientras que, en la figura IV14B, se observa cómo queda en la configuración, de acuerdo con la respuesta a la solicitud "sh run".

```
Pue#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Pue(config)#router rip
Pue(config-router)#version 2
Pue(config-router)#network 8.0.0.0
Pue(config-router)#exit
Pue(config)#exit
```

(A)

```
!
router rip
 version 2
 network 8.0.0.0
 network 10.0.0.0
!
ip classless
!
```

(B)

Fig. IV.14. A) Configuración para RIPv2 en el *router* Pue. B) Resultado vía Sh run

En la simulación de la figura IV.15, podemos observar que ya se reconocen los paquetes RIPv2, llegando, desde el *router* CDMX, al *router* Puebla y al *switch* de la red 192.168.1.0, como se indica en la figura IV.15.

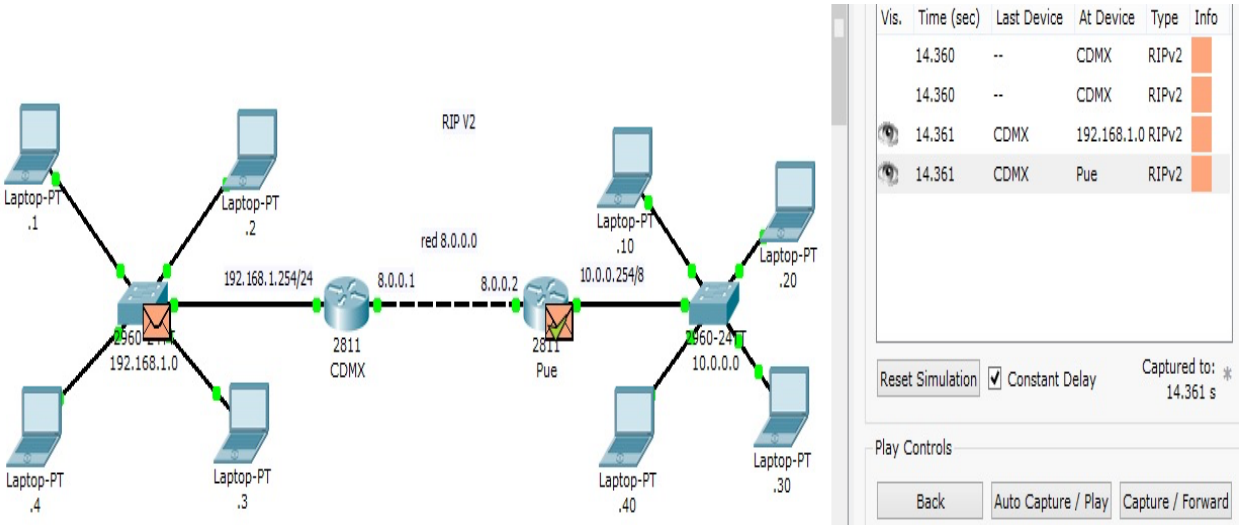


Fig. IV.15. Captura de la simulación en la que los paquetes RIPv2 salen del *router* CDMX.

Mientras que, en la figura IV.16, se muestran los detalles para el paquete RIPv2 que llegó al router Pue. En RIPv2, la dirección destino será **MULTICAST 224.0.0.9**, con la finalidad de evitar las direcciones de clases A, B y C. También se observan los detalles de *route tag*, *subnet* y *next hop* que no aparecían en RIPv1, pero que se indicaron en el formato RIPv2 de la figura III.4

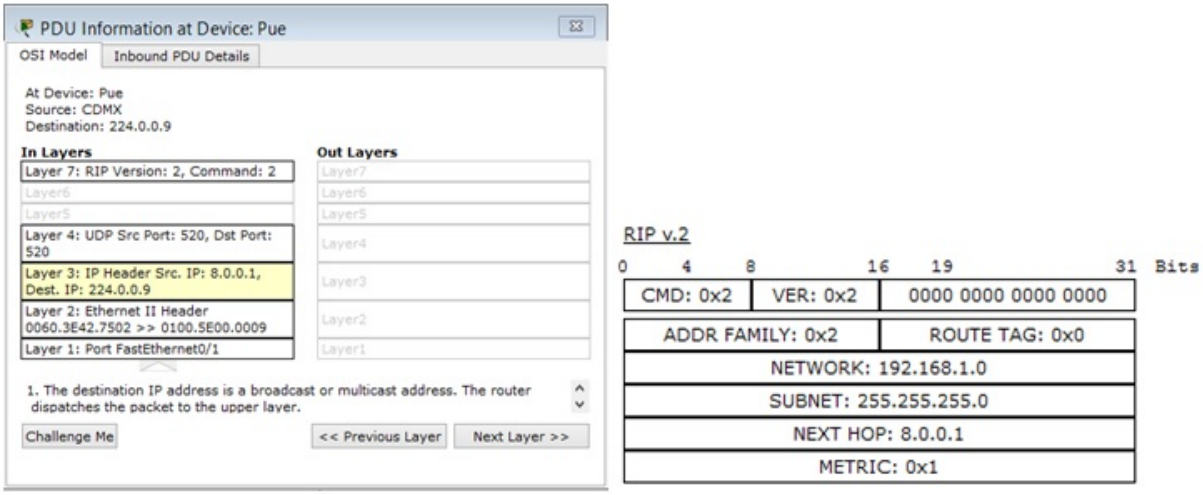


Fig. IV.16. Detalles del paquete RIPv2 que ha llegado al *router* Pue, desde el CDMX.

Para evitar que los paquetes RIP que van hacia los *hosts* se queden como tráfico inútil y se desechen, debemos agregar, a la configuración de la interfaz en cuestión, la orden “pasive-interface gig0/0”, y así RIP la identifica como una red pasiva, evitando ese tráfico excedente.

IV.5 OSPF

El *Open Shortest Path First* (OSPF) es un protocolo de enrutamiento de estándar abierto, el cual emplea el algoritmo *Shortest Path First* (SPF), de Dijkstra, para propiciar una mejor convergencia en la red respecto del resto de los protocolos existentes. Debido a que es un estándar abierto, éste se puede implementar para diferentes plataformas. Los fabricantes, por lo general, agregan a la base características extendidas, por lo que, en ocasiones, algunas funciones podrían no ser soportadas entre distintos fabricantes. OSPF fue diseñado para ejecutarse dentro de un AS, por lo que es un IGP, en el que cada *router* mantiene una base de datos idéntica, la cual describe la topología del AS y, a partir de esa BD, se infiere una tabla de *ruteo o enrutamiento,* vía la construcción del *Shortest Path Tree* (SPT).

La versión 1 de OSPF apareció, en 1989, bajo el RFC 1131, sin embargo, nunca se implementó **[24]**.

La versión 2 de OSPF se creó, en 1991, bajo el RFC 1247 y RFC 1248, sus mejoras están en los RFC 1583, RFC 2178 y, finalmente, como estándar de Internet en el RFC 2328 de 1998. Cabe mencionar que OSPF es uno de los protocolos soportados por la tecnología MPLS (*Multi-Protocol Label Switching*) **[25-29]**.

Las versiones OSPFv1 y OSPFv2 describen al protocolo bajo IPv4, mientras que OSPFv3 bajo el IPv6, vía el RFC 2740 y su actualización con el RFC 5340 **[30-31]**. Para los interesados en el protocolo IPv6, este se trata en el capítulo VIII.

Características de OSPF:

1. Emplea áreas, lo cual permite usar muchas redes y jerarquizarlas. En este caso un *router* de núcleo (*Backbone Router* - BR) es aquel que se encuentra dentro del "área 0", mientras que, en un *router* interno (*Internal Router* - IR), sus interfaces están conectadas dentro de un área diferente al área 0. Para interconectar las distintas áreas, se emplean los *router* de frontera de área *(Area Border Router* – ABR) y, para interconectar un AS con otro, se emplean los *router* de enlace de sistema autónomo (*Autonomous System Boundary Router* - ASBR). En este caso, un *router* OSPF se conecta a un proceso de enrutamiento externo, el cual intercambia información con ese proceso. Todos estos tipos de *routers* se muestran, de acuerdo con la función descrita en el diagrama de la figura IV.17.
2. Emplea una base de datos de enlace-estado para eliminar los posibles "bucles de enrutamiento", lo que hace que la red tenga una convergencia rápida.

3. Soporta un comportamiento de enrutamiento sin clases.
4. Usa un resumen de rutas para reducir el tamaño de las tablas de enrutamiento.
5. Reduce el ancho de banda requerido, al enviar las actualizaciones de las rutas solamente cuando es requerido.
6. Emplea paquetes direcciones *multicast* (224.0.0.5 y 224.0.0.6), para reducir el impacto en los equipos y *routers* que no estén activos en un determinado momento.
7. Soporta autenticación para hacer más seguras las redes.

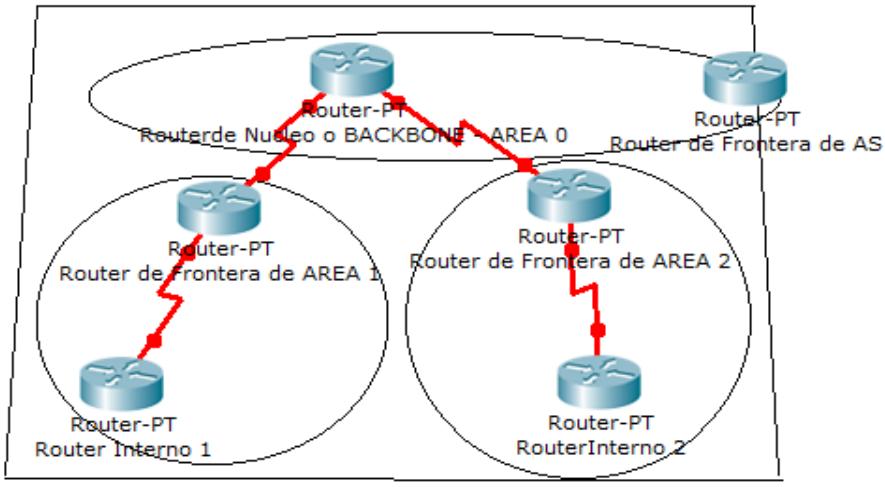


Fig. IV.17 Distintas denominaciones de *routers* dentro y fuera de un AS OSPF.

IV.5.1 Evolución de OSPF

A manera de resumen, la evolución de OSPF se indica en la tabla IV.2.

Proposed Standard	Draft Standard	Internet Standard
OSPF v1		
RFC 1131-1989 (experimental) The OSPF specification		
OSPF v2		
	RFC 1247-1991	
RFC 1248-1992	RFC 1583-1994	
	RFC 2178-1997	RFC 2328-1998
OSPF v3		
RFC 2740-1999 (Dic)		
RFC 5340-2008		

Tabla IV.2 Evolución del estándar OSPF.

IV.6 Paquetes OSPF

Los paquetes OSPF contienen 9 campos: *Version number, Type (Data type - tipo de dato), Packet length (bytes), Router ID (source-fuente* del paquete*), Area ID (source-fuente* del paquete*), Checksum, authentication type, Authentication y Data*.

En el caso de los mensajes, pueden existir 5 tipos de mensajes:

Tipo 1: Hello, el cual sirva para reconocer a los *routers* vecinos.

Tipo 2: Descripción de la base de datos (*Data Base Description* - DBD), el cual contiene un resumen de la base de datos de los enlaces de estado.

Tipo 3: Requerimiento del estado del enlace (*Link State Requirement* - LSR).

Tipo 4: Actualización del estado del enlace (*Link State Update* – LSU).

Tipo 5: Reconocimiento del estado del enlace (*Link State Acknowledment* - LSAck).

Version (1)	Type [1-5] (1)	Packet Length (2)
Router ID (4)		
Area ID (4)		
Checksum (2)		Authentication Type [0-1] (2)
Authentication [0-1] (8)		
Network Mask (4)		
Hello Interval (1)	Options (1)	Router Priority (2)
Router Dead Interval (4)		
Designated Router (4)		
Backup Designated Router (4)		
Neighbor Count (4)		

Fig. IV.18 (a) Paquete OSPFv2, mensaje *HELLO*. Encabezado de 24 bytes.

Características OSPFv2

El paquete para la versión 2 no cambió su encabezado.

Para “Versión”: 1 versión 1, 2 versión 2.

Para “Type”: 1 Hello, 2 DBD, 3 LSR, 4 LSU y 5 ACK.

Para “Authentication Type”: 0 (sin password), 1 (password simple).

“Hello interval”, segundos entre paquetes *hello.*

“Router Dead Interval”, segundos para designar la muerte de un *router.*

Para “Router priority”, 0 equivale a que el *router* no es elegible como *backup.*

Para “Designated Router”, 0 equivale a que no hay un DR.

Para “Backup Designated Router”, 0 equivale a que no hay un BDR.

Mensajes HELLO

En un simulador, al paquete OSPF v2 tipo 1, o mensaje HELLO, se lo muestra en la figura IV.19.

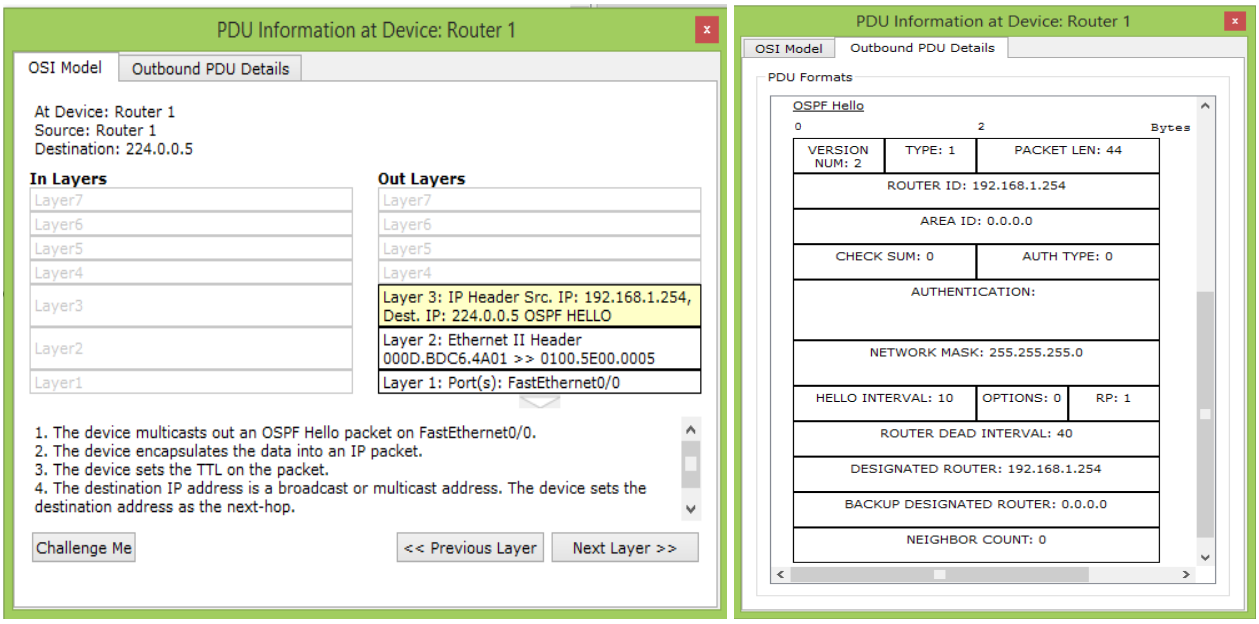


Fig. IV.19 (a) Paquete OSPFv2 tipo 1. (b) Mensaje HELLO en simulador.

Mensajes DBD

En la figura IV.20, se observan los detalles del paquete OSPFv2 tipo 2, el mensaje DBD, donde el encabezado muestra que 1500 bytes es el tamaño *default* para las tramas, que se reciben y transmiten en todas las interfaces, indicadas como MTU (*Maximum Transmission Unit*), pero que se podrían usar MTU Jumbo de 7500. Se observa la descripción de una tabla llamada Cisco *Express Forwarding* (CEF), misma que sólo es propietaria de Cisco.

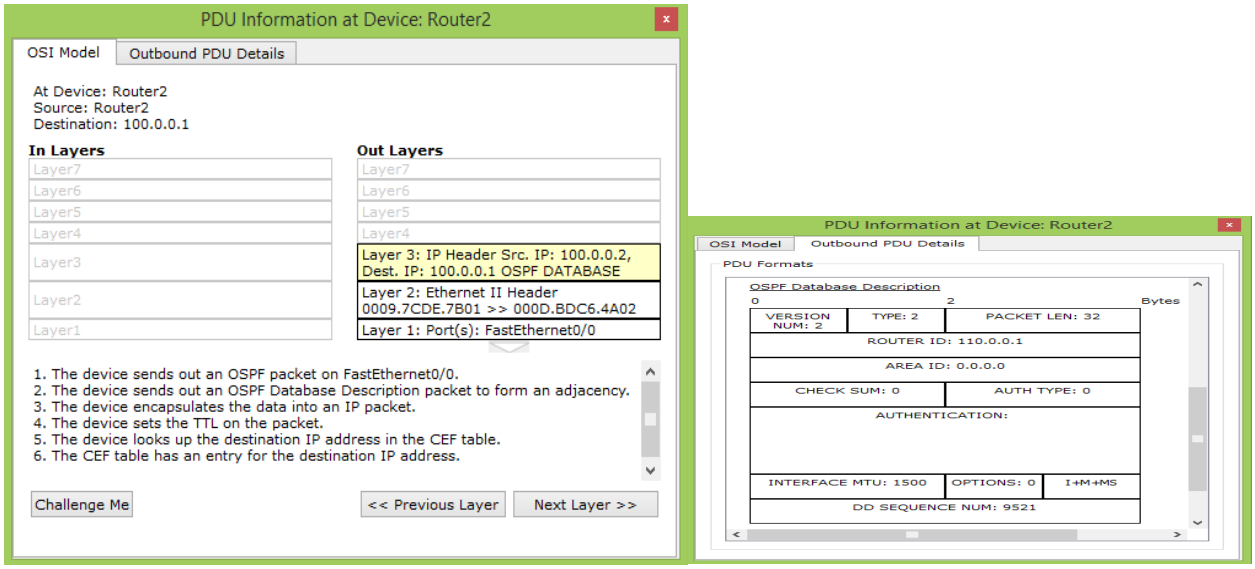


Fig. IV.20 (a) Paquete OSPFv2 tipo 2. (b) Mensaje DBD.

Mensajes LSR

El paquete OSPFv2 del tipo 3, el mensaje LSR, se observa en el simulador como en la figura IV.21.

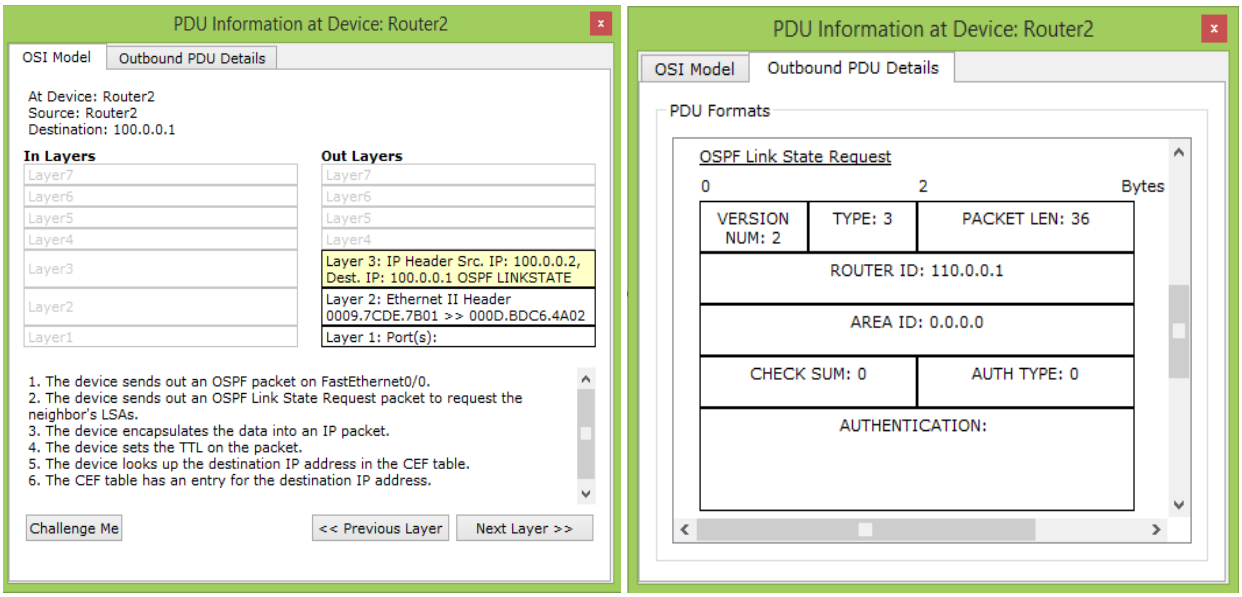


Fig. IV.21 (a) Paquete OSPFv2 tipo 3. (b) Mensaje LSR.

Mensajes LSU

Al paquete OSPFv2 del tipo 4, el mensaje LSU, se observa en el simulador como en la figura IV.22.

En este paquete se incluyen los anuncios del estado del enlace (*Link State Advertisement* - LSA).

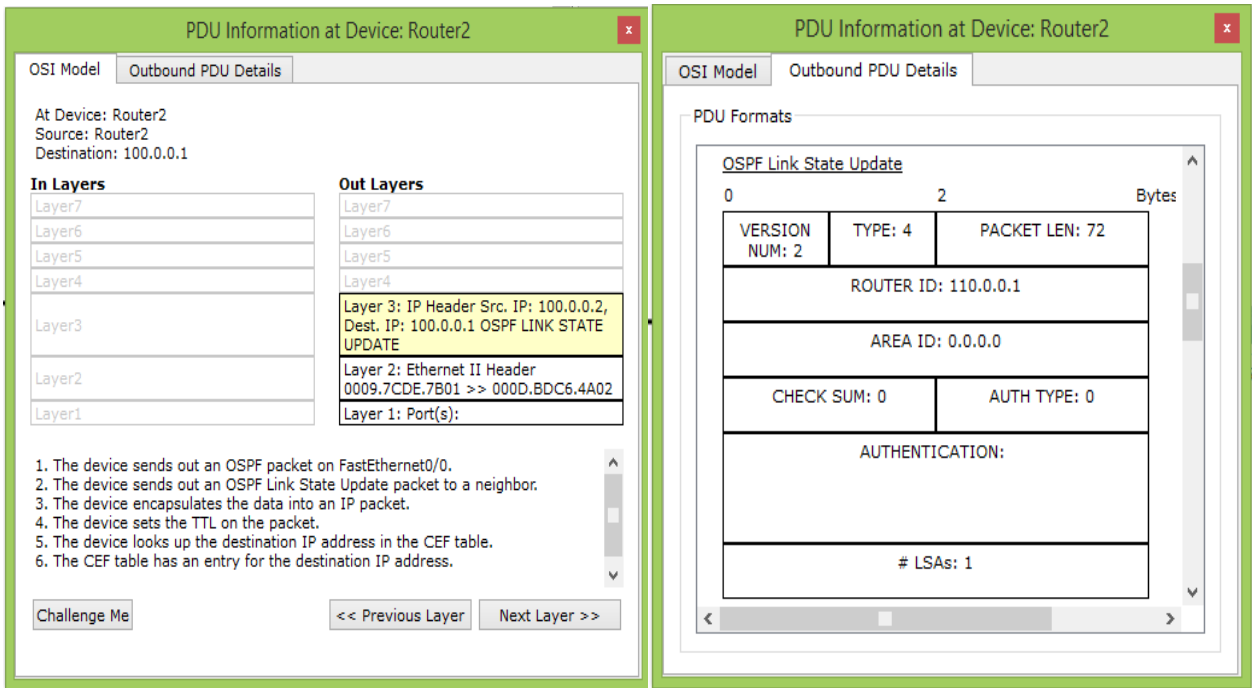


Fig. IV22 (a) Paquete OSPFv2 tipo 4. (b) Mensaje LSU.

Mensajes LSAck

En un simulador, al paquete OSPF v2 del tipo 5, el mensaje LSAck, se detalla en la figura IV.23.

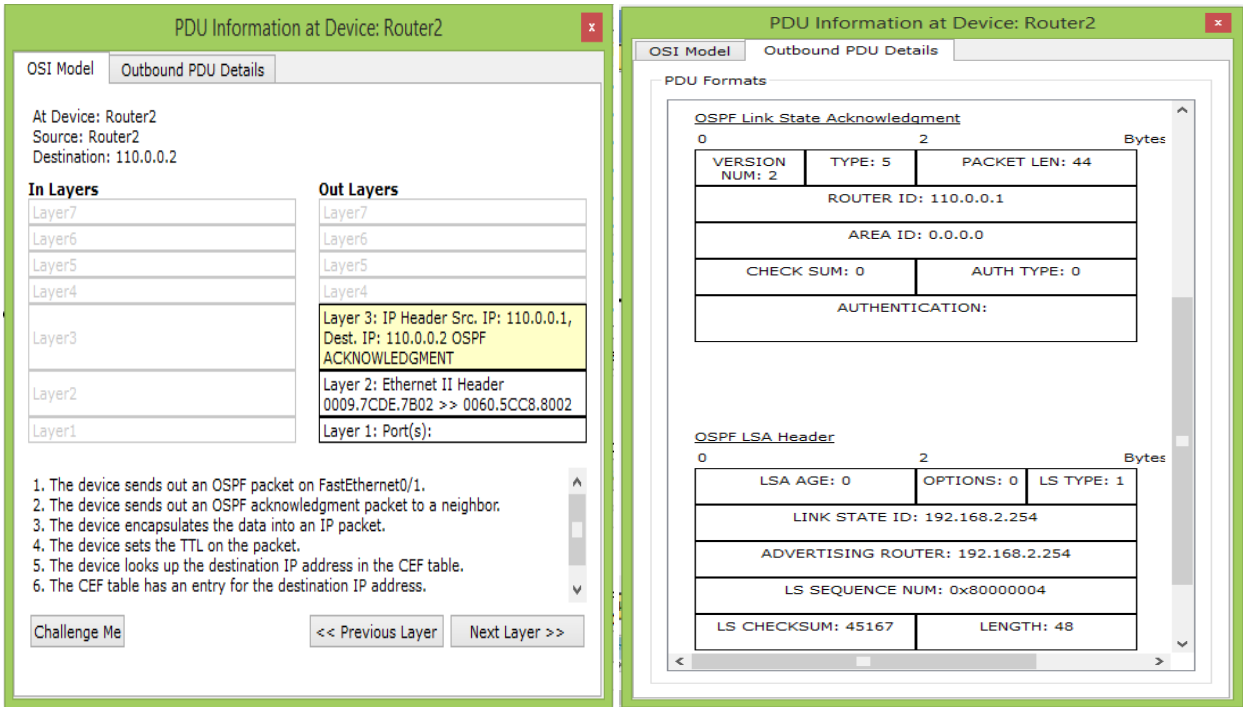


Fig. IV.23 (a) Paquete OSPFv2 tipo 5. (b) Mensaje LSAck.

Wildcard

En la tabla IV.3, se muestra la correspondencia entre la máscara de subred y la *wildcard,* las cuales son necesarias a la hora de configurar OSPF.

	Binario	**Decimal**
Máscara natural de subred clase A	11111111.00000000.00000000.00000000	255.0.0.0
Wildcard	**00000000.11111111.11111111.11111111**	**0.255.255.255**
Máscara natural de subred clase C	11111111.11111111.11111111.00000000	255.255.255.0
Wildcard	**00000000.00000000.00000000.11111111**	**0.0.0.255**

Tabla IV.3 Máscara y su correspondiente Wildcard.

IV.7 Redes con OSPFv2

Considere que la topología de red de la figura IV.24 fue configurada con el protocolo de enrutamiento OSPFv2, cuyo paquete OSPF se indica como un sobre azul.

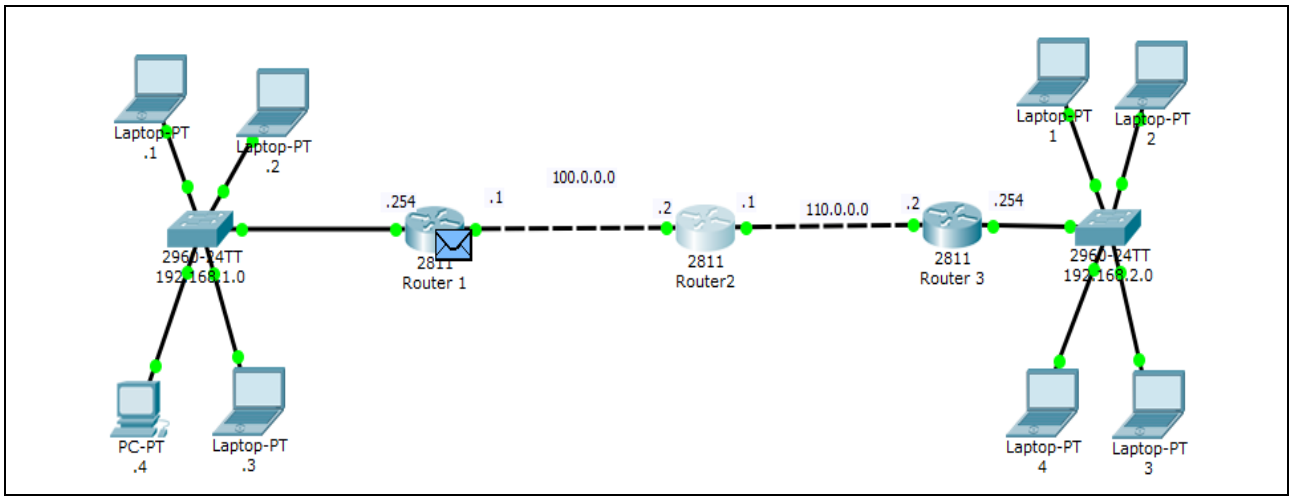


Fig. IV.24 Topología con 4 redes, 3 *routers* configurados bajo OSPFv2.

Para la configuración se debe indicar el número de proceso, el cual es un número entero arbitrario bajo el formato "router / ospf / **proceso"** y el área cero corresponde al *backbone, como se indica en la segunda línea "*network/ip de red/(WILDCARD) **inverso de máscara de subred**/area/0". La configuración se realiza como se indica en la figura IV.25

```
Router2(config)# router ospf 10
Router2(config-router) #network 100.0.0.0 0.0.0.255 area 0
Router2(config-router) #network 110.0.0.0 0.0.0.255 area 0
```

Fig. IV.25 Configuración de un router bajo OSPFv2.

Una vez que se han compartido los paquetes OSPF, con sus 5 tipos de mensajes, todos los *routers* tienen completas sus tablas de enrutamiento. La figura IV.26 muestra la tabla de enrutamiento para el *router* 2; en ella se observan las redes contiguas al *router* 2 y las otras 2 redes, que conoce gracias al protocolo OSPF.

Veamos, a detalle, otro ejemplo en la configuración de la figura IV.27

```
Router2#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
C    110.0.0.0/8 is directly connected, FastEthernet0/1
O    192.168.1.0/24 [110/2] via 100.0.0.1, 00:01:00, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 110.0.0.2, 00:01:00, FastEthernet0/1
```

Fig. IV.26 Tabla de enrutamiento para el *router* 2.

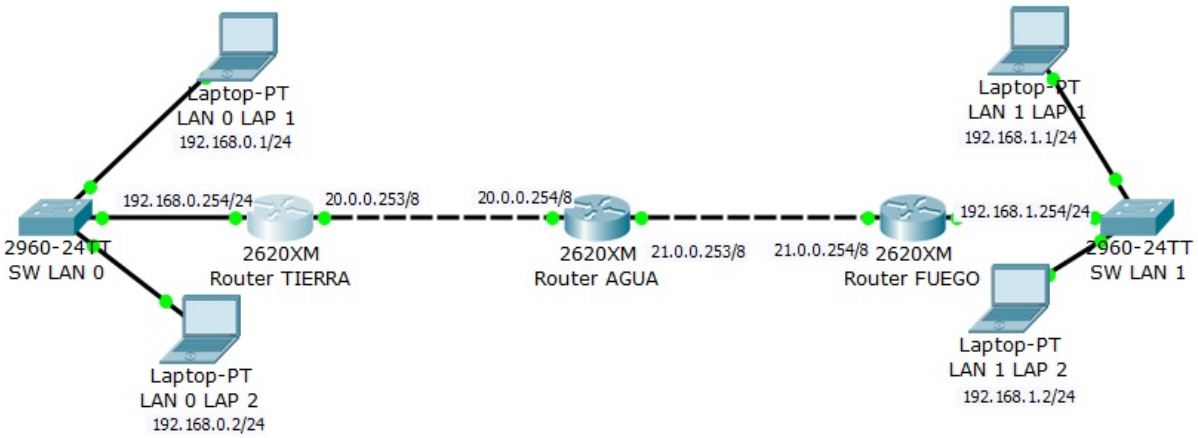


Fig. IV.27 Segunda topología con 4 redes y 3 *routers* configurados bajo OSPFv2.

Al solicitar la configuración del *router* Tierra la respuesta se obtiene en la figura IV.28.

```
TIERRA# sh run
Building configuration...
Current configuration: 676 bytes
version 12.2
hostname TIERRA
ip cef
no ipv6 cef
interface FastEthernet0/0
ip address 20.0.0.253 255.0.0.0
duplex auto
speed auto
interface FastEthernet1/0
ip address 192.168.0.254 255.255.255.0
duplex auto
speed auto
router ospf 2
log-adjacency-changes
network 20.0.0.0 0.255.255.255 area 0
ip classless
ip flow-export version 9
login
end
```

Fig. IV.28 Configuración que se está ejecutando en el *router* Tierra.

Por su parte, la figura IV.29, muestra la tabla de enrutamiento previa a la difusión de los 5 tipos de paquetes OSPF.

```
TIERRA# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set

C 20.0.0.0/8 is directly connected, FastEthernet0/0
C 192.168.0.0/24 is directly connected, FastEthernet1/0
```

Fig. IV.29 Tabla de enrutamiento sin haberse ejecutado y distribuido paquetes OSPFv2.

Obsérvese que, si bien el *router* Tierra ya se ha configurado, el *router* Agua todavía no "habla el idioma OSPF", por lo cual descarta los paquetes OSPF. Esta acción es detectada por el simulador marcándolo con un tache rojo, como se indica en la figura IV.30. Sólo hasta que se configura correctamente cada uno de los mensajes de OSPF, se va difundiendo hasta que se llenan las tablas de enrutamiento. Pero veamos, paso a paso, este proceso.

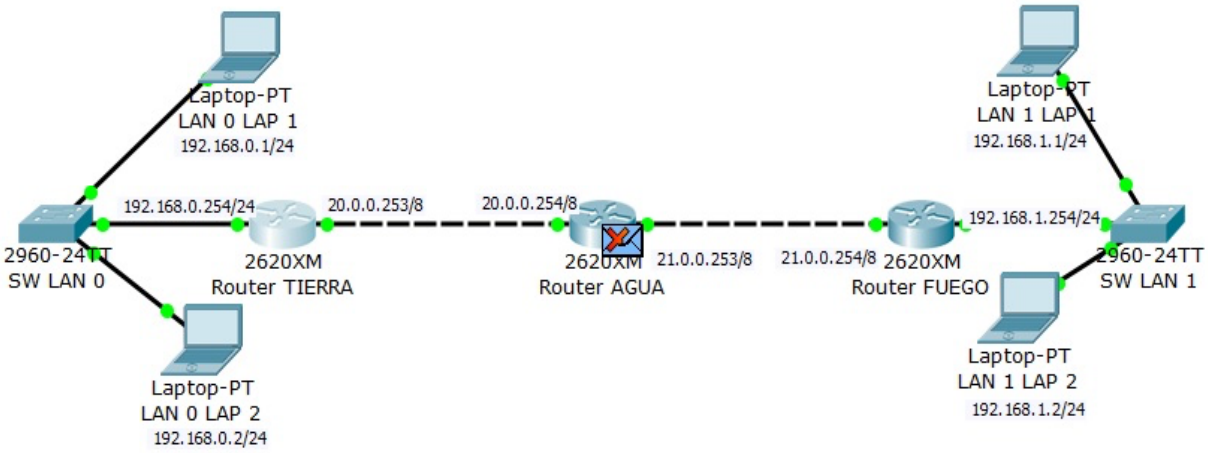


Fig. IV.30 Descartado de paquetes OSPFv2 en el *router* Agua.

Entonces, para configurar al *router* Agua, se realiza la configuración indicada en la figura IV.31, en la que el proceso es "100" y se indican las dos redes contiguas al *router* Agua sobre las que se quiere hablar el protocolo OSPFv2. De manera similar se configura el *router* Fuego.

```
Agua(config)#router ospf 100
Agua(config-router) #network 20.0.0.0 0.255.255.255 area 0
Agua(config-router) #network 21.0.0.0 0.255.255.255 area 0
Agua(config-router) #
```

Fig. IV.31 Configuración del protocolo OSPFv2 sobre el *router* Agua.

Una vez configurado correctamente el *router* Agua, la figura IV.32 muestra cómo se han difundido los paquetes OSPF *Hello*, los mensajes DBD (indicados con un paquete en azul marino). Se van completando los 5 tipos de mensajes y se van llenando las tablas de enrutamiento, las cuales vemos en la figura IV.33. Observe todos los detalles.

En cada *router* se dan de alta las cuatro redes: dos contiguas para cada *router* y dos que se conocen gracias al protocolo OSPFv2.

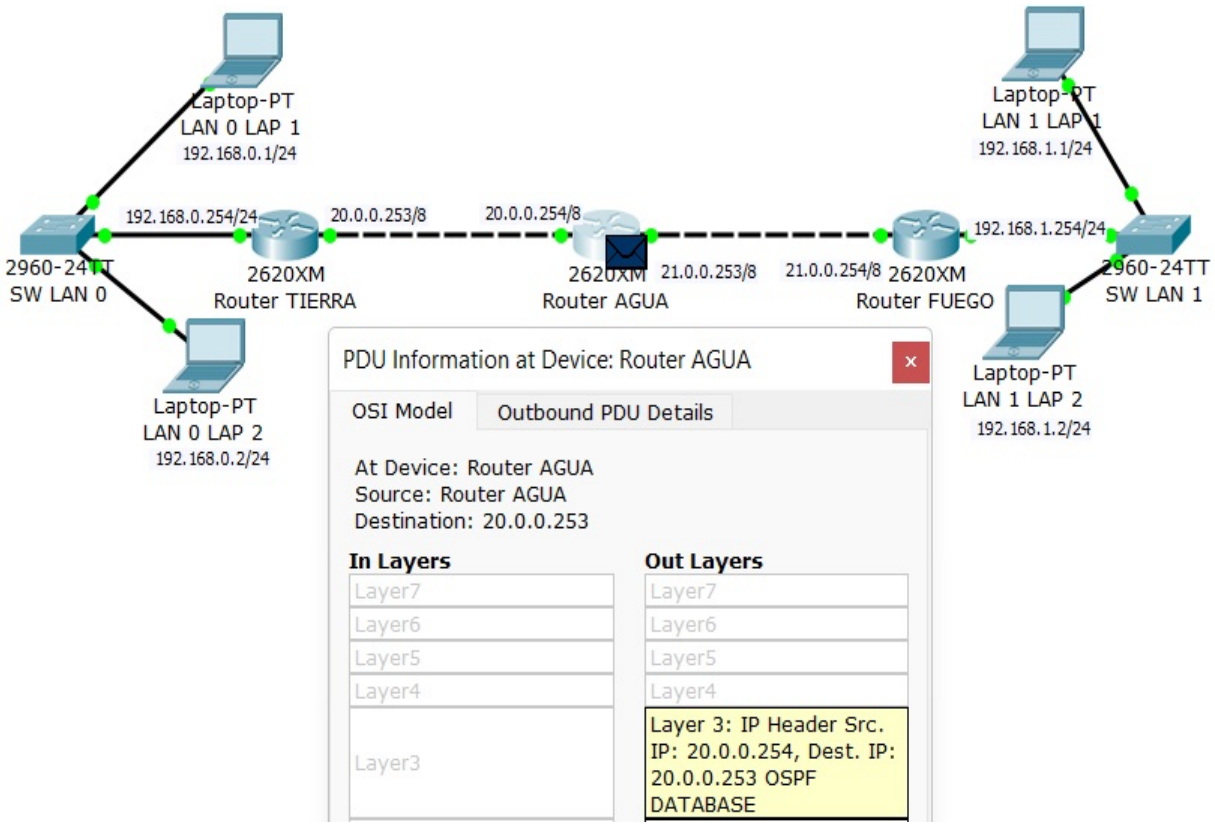


Fig. IV.32 Paquetes OSPFv2 DBD en el *router* Agua, en el proceso de llenado de las tablas de enrutamiento.

TIERRA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
* - candidate default, U - per-user static route, o - ODR
Gateway of last resort is not set

C 20.0.0.0/8 is directly connected, FastEthernet0/0
O 21.0.0.0/8 [110/2] via 20.0.0.254, 00:05:10, FastEthernet0/0
C 192.168.0.0/24 is directly connected, FastEthernet1/0
O 192.168.1.0/24 [110/3] via 20.0.0.254, 00:00:25, FastEthernet0/0

Agua#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
Gateway of last resort is not set

C 20.0.0.0/8 is directly connected, FastEthernet0/0
C 21.0.0.0/8 is directly connected, FastEthernet1/0
O 192.168.0.0/24 [110/2] via 20.0.0.253, 00:00:25, FastEthernet0/0
O 192.168.1.0/24 [110/2] via 21.0.0.254, 00:00:25, FastEthernet1/0

Fuego#sh ip route
%SYS-5-CONFIG_I: Configured from console by console

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
Gateway of last resort is not set

O 20.0.0.0/8 [110/2] via 21.0.0.253, 00:05:10, FastEthernet0/0
C 21.0.0.0/8 is directly connected, FastEthernet0/0
O 192.168.0.0/24 [110/3] via 21.0.0.253, 00:00:25, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet1/0

Fig. IV.33 Tabla de enrutamiento para los 3 *routers*.

Finalmente, se realizan pruebas de conectividad enviando un *ping*, entre las computadoras de los extremos, y se observan tanto el flujo de los paquetes OSPFv2 tipo *Hello* (azules), entre los *routers*, como el flujo bidireccional de paquetes ICMP (morados) que van desde una computadora a la otra y de regreso, como se indica en la figura IV.34. Una vez que se han completado las tablas, los *routers* sólo emiten paquetes OSPFv2 del tipo “Hello” y se da el proceso de los cinco mensajes hasta que existe algún cambio en la topología de la red.

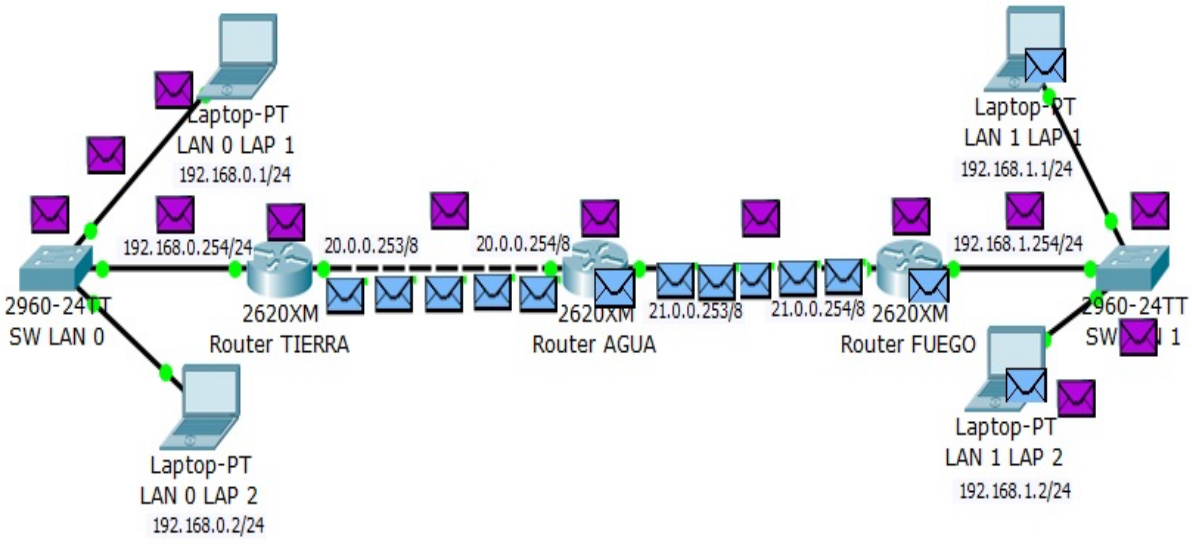


Fig. IV.34 Prueba de conectividad vía paquetes ICMP y protocolo de enrutamiento vía paquetes OSPFv2

IV.8 PRÁCTICA 5 - Enrutamiento dinámico RIP y OSPF

Dada la figura IV.35, realice las simulaciones indicadas en las actividades 1 y 2. El circuito consta de 9 redes y 8 *routers*.

Actividad 1: RIP. Configure con base en el protocolo RIP y compruebe la conectividad total.
Actividad 2: OSPF. Configure con base en el protocolo OSPF y compruebe la conectividad total.

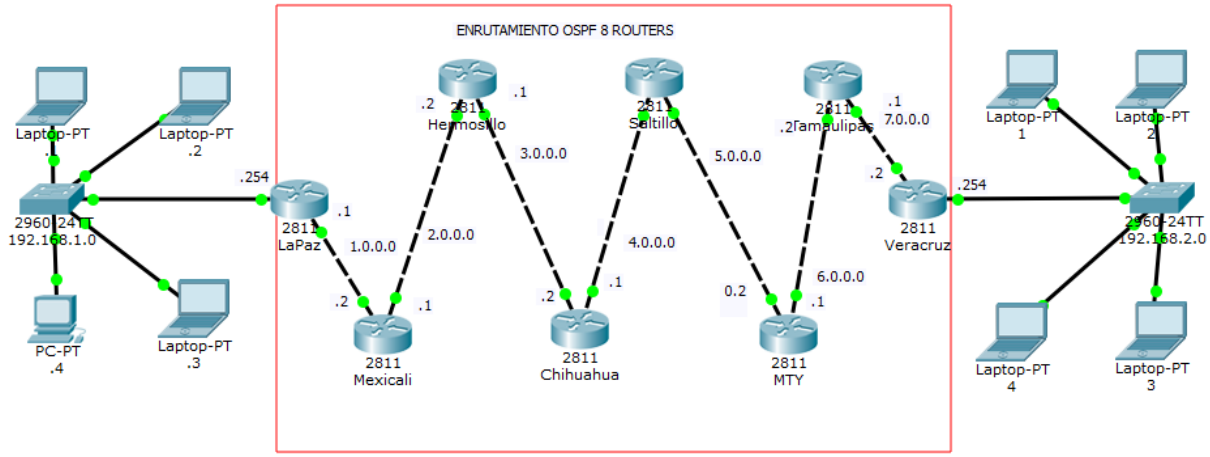


Fig. IV.35 Topología física para 9 redes con 8 *routers*: Caso México.

Dada la figura IV.36, realice las simulaciones indicadas en las actividades 3 y 4.

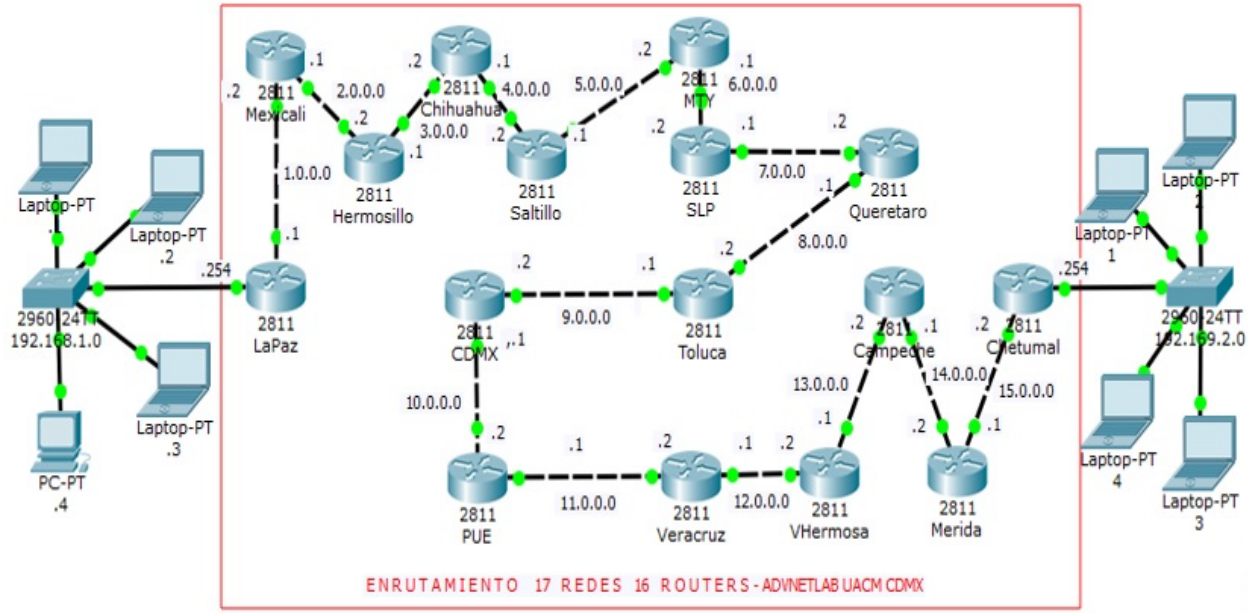


Fig. IV.36 Topología física para 17 redes con 16 *routers*: Caso México.

Actividad 3: RIP. Configure con base en el protocolo RIP y compruebe la conectividad total.
Actividad 2: OSPF. Configure con base en el protocolo OSPF y compruebe la conectividad total.

IV.9 EVALUACIÓN PARTE II

SECCIÓN I: Enrutamiento - conceptos básicos

1.Describa la función de un *router* [1p]

_____
_____
_____

2. Indique al menos 5 modelos comerciales de *routers* [1p]

A)_____B)_____C)_____
D)_____E)_____

3. Enliste al menos 5 procesadores o controladores empleados en *routers* [1p].

A)_____B)_____C)_____
D)_____E)_____

4. Indique cuál es el criterio usado por los fabricantes de *routers* para determinar la obsolescencia de un producto [1p].

_____

5. Señale la diferencia entre enrutamiento estático y dinámico [1p]

_____
_____

SECCIÓN II: Infraestructura

6.Expanda (sin traducir) los acrónimos relacionados con infraestructura de red [1p]
IDF_____
MDF_____
SAN_____

7. **Indique** la diferencia entre cableado horizontal y vertical [1p]

_____
_____

8.Indique el estándar que define los cables y sus características para el "cableado estructurado" [1p]._____
9.Metro Ethernet fue posible gracias al desarrollo de estándares, conformando PBB y PBN, con lo cual se introdujeron nuevos formatos de trama para usar B-MAC, correspondientes a los BEB. **Indique** el estándar que hizo posible la integración de actualizaciones y escalabilidad para hacer, a su vez, posible Metro Ethernet [1p]._____

10.Explique a qué se le llama "Carrier Ethernet" [1p]

_____

_____

SECCIÓN III: Enrutamiento estático y dinámico

Problema 1: Con base en el circuito de la figura IV.37, suponga que se encuentra en contacto con la CLI del *router* y que las bases de datos de los *switches y router* están vacías.

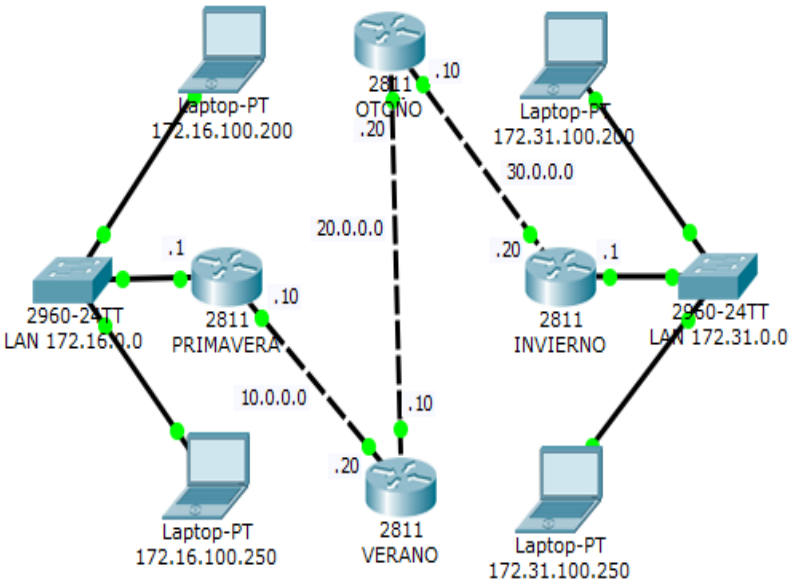


Figura IV.37. Cinco redes cuatro routers

1. Configure el *router* OTOÑO con base en enrutamiento estático [2p]

```
OTOÑO(config)#
```

2. Muestre la tabla de ruteo para el *router* OTOÑO [2p]

Problema 2: Con base en el circuito de la figura IV.37, suponga que se encuentra en contacto con la CLI del *router*, y que las bases de datos de los *switches y router* están vacías. Usted configura los *routers* con base en RIPv2

3. Mostrar la tabla de *enrutamiento* para el *router* OTOÑO [2p]

Problema 3: Con base en el circuito de la figura IV.37, suponga que se encuentra en contacto con la CLI del *router*, las bases de datos de los *switches y router* están vacías. Usted configura los *routers* con base en OSPFv2.

4. Muestre la tabla de *enrutamiento* para el *router* OTOÑO [2p]

5. Muestre los formatos para los paquetes RIPv2 [1p] y para OSPFv2 (Hello) [1p]

Paquete RIPv2 Paquete OSPFv2

PARTE III: INFRAESTRUCTURA Y GESTIÓN DE RED

CAPÍTULO V: INFRAESTRUCTURA DE LAS REDES

La infraestructura de las redes pequeñas, medianas, grandes o la Internet, son el equivalente a los sistemas de agua, energía eléctrica, alumbrado, carreteras, ferrocarriles o aeropuertos en una ciudad; cuando funcionan bien nadie lo nota, pero, cuando colapsan, recordamos nuestra fragilidad como especie. La infraestructura de la Internet permitió un cambio civilizatorio y la transición de la tercera, a la cuarta revolución industrial, de 1983 a 2000, pero, paradójicamente, con ella inició la tercera guerra global de corte pluri o multidimensional en 2010. La infraestructura de Internet fue el escenario del inicio de la ciberguerra al destruir infraestructura crítica física, luego permitió trasladar las guerras económicas, políticas, sociales y culturales al plano de la información, incluyendo la inteligencia y la contrainteligencia convencionales, posteriormente llegaron las guerras científicas, espaciales y comerciales, hasta llevarnos a una nueva guerra fría física en 2022 y …

V.1 Infraestructura de una red de datos MAN

Con la finalidad de ejemplificar la distribución de la infraestructura de telecomunicaciones que soporta servicios de voz, datos y video, en una institución hipotética, pública o privada, supongamos que cuenta con 7 localidades distribuidas en distintos puntos de una ciudad, como se muestra en la figura V.1. La comunicación a internet se realiza mediante 6 enlaces E1 a 2 Mbps y un enlace E3 a 12 Mbps (34Mbps dividido entre 3), proveídos por algun ISP (*Internet Service Provider*). La salida se hace mediante *routers* Cisco 3845, y se tiene salida a internet vía 32 IP públicas.

Cada una de las sedes se enlaza por radiocomunicación, vía antenas independientes. La institución cuenta con 2,345 computadoras, 32 servidores físicos Proliant MLS70 y Dell T600SC, todos con procesadores Intel Xeon y 1,300 extensiones telefónicas, con equipos Avaya. Se cuenta con 100 switches. De ellos 7 son *core switches* marca Extreme Networks, modelo Black Diamond 8810. Y están ubicados en la instalación de distribución principal (*Main Distribution Facility* - MDF) de cada sede. El resto son switches de agregación de las marcas Extreme Networks, modelo Summit 450 (73), Alcatel (15) y Nortel Baystack 460 (5); todos ellos se encuentran en la instalación de distribución intermedia (*Intermediate Distribution Facility* - IDF) **[1]**.

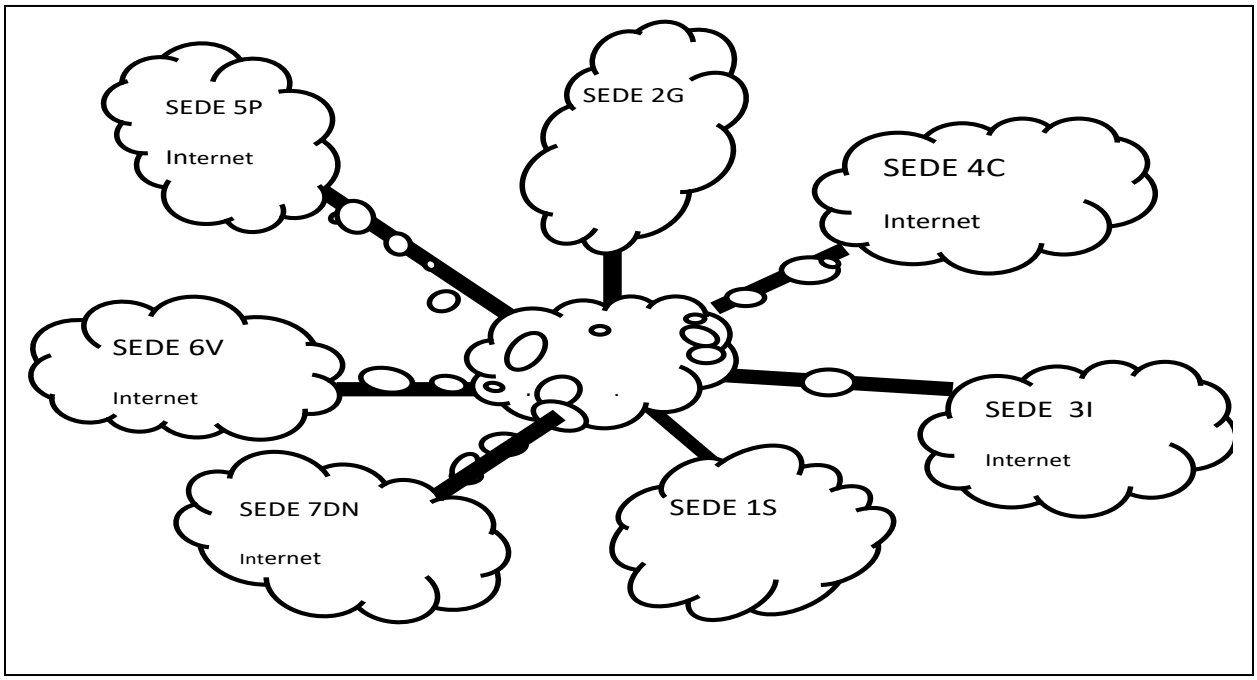


Fig. V.1. *Topología de telecomunicaciones MAN en una institución, cada sede constituye una LAN.*

El cableado que va desde una MDF a una o varias IDF se conoce como **cableado vertical**, mientras que el cableado que se distribuye desde las IDF a los *End Systems* se le llama **cableado horizontal**. Tales nombres se desprenden del hecho de que, en un principio, se contaba con un MDF por edificio y en cada piso había un IDF, lo cual requería un cableado vertical entre pisos; mientras que el cableado entre el IDF y las computadoras e impresoras se hacía en el mismo piso, de allí en nombre de cableado horizontal.

En la tabla V.1 se resume la distribución de la infraestructura en las distintas sedes. La red MAN se configuró de tal modo que cuenta con 70 VLAN y en el MDF, de la sede 1, se puede contar con una Red de área de almacenamiento (*Storage Area Network* - SAN*)* de 20 TB **[32]**.

Sedes	Core switches	Access switches	Líneas para voz	% uso internet
1 (S) / E3	1	24	435	18 %
2 (G) / E1	1	14	140	71 %
3 (I) / E1	1	9	112	74 %
4 (C) / E1	1	7	122	69 %
5 (P) / E1	1	10	154	94 %
6 (V) / E1	1	6	189	85 %
7 (DN) / E1	1	4	145	78 %

Tabla V.1 Infraestructura de institución distribuida en 7 sedes.

Cabe aclarar que Nortel Networks fue comprado en 2009 por AVAYA, de modo que los equipos Nortel cayeron, de inmediato, en obsolescencia.

La figura V.2 muestra instalaciones parciales de un MDF.

Fig. V.2. En un MDF: Servidores EMC^2, piso falso, sistema Lieber de refrigeración.

La figura V.3a muestra un *rack* expuesto con *switches* de acceso, ubicado en un IDF (observe la disposición desordenada de los cables, lo que se considera una mala práctica); mientras que la V.3b muestra a un rack en gabinete con puerta, el cual sigue estándares de cableado estructurado (lo que se considera buena práctica ya que el ordenamiento de cables permite una fácil identificación de fallas y, en su caso, la solución de problemas).

Fig. V.3. Rack dentro de un IDF. A) Cableado desordenado. B) Cableado según estándares (2021)

La figura V.4 muestra un diagrama de la distribución de switches de agregación o acceso en un rack ubicado en un IDF. En este caso la topología muestra 2 IDF, los cuales se conectan a un MDF, correspondiente a la sede 5.

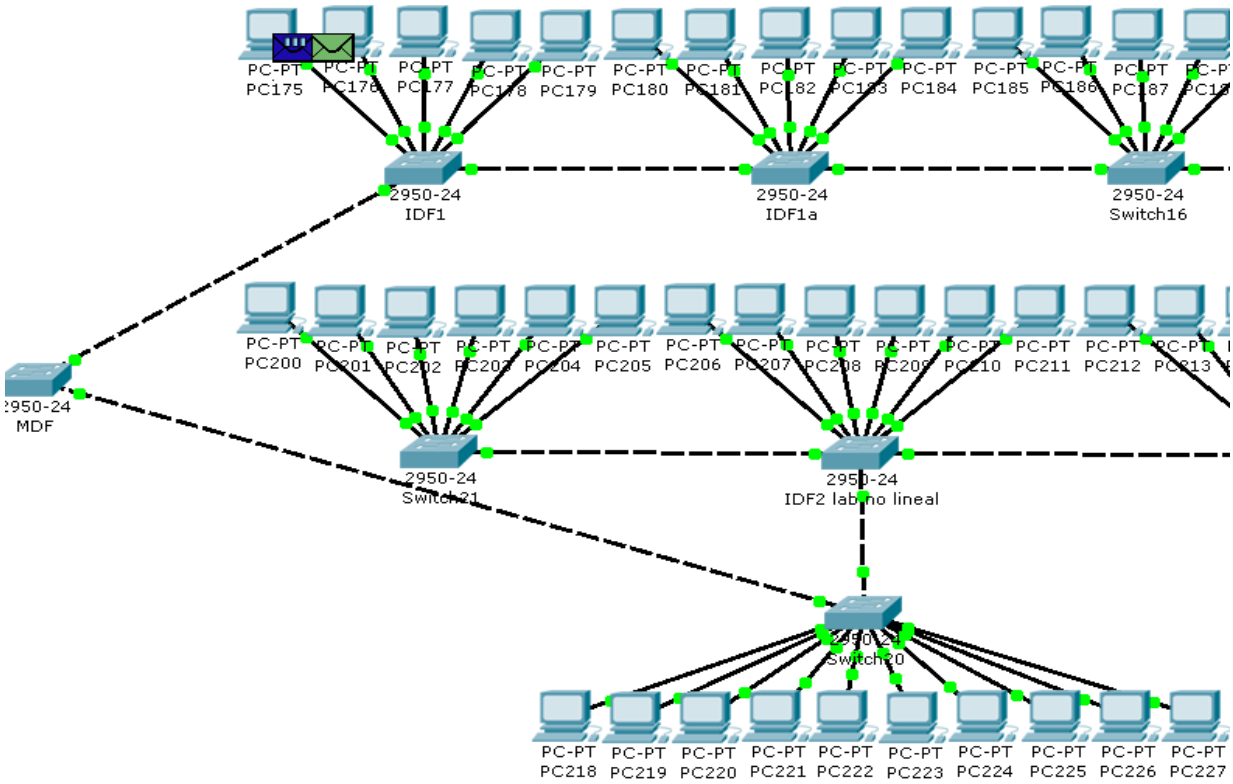


Fig. V.4. Topología física de interconexión entre switches en dos IDF conectados a su *core-switch* en el MDF.

Por su parte la figura, V.5 muestra la topología correspondiente a la sede 1, en la cual 8 IDF se comunican con el MDF [33].

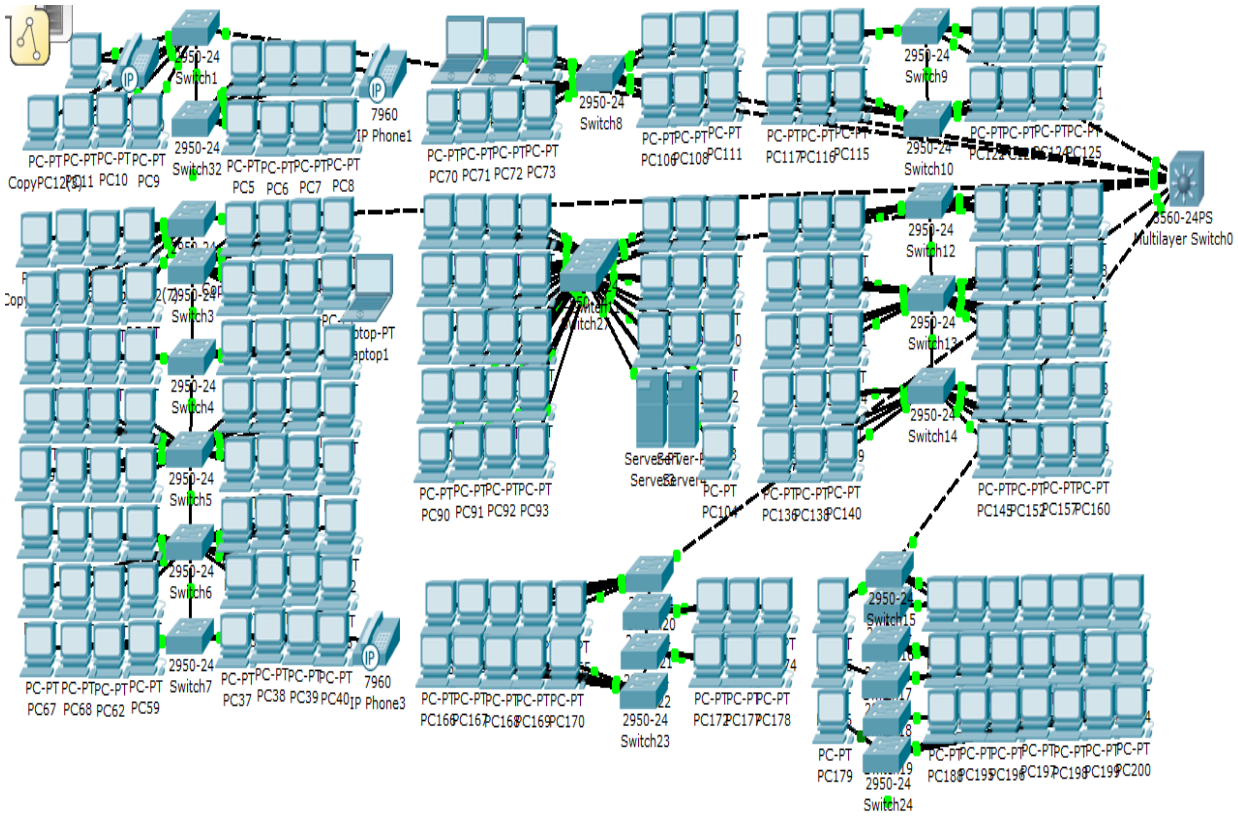


Fig. V.5. Simulación de la infraestructura para el campus SLT con sólo 200 hosts conectados a 8 IDF.

V.2 *Data Centers* y estándares internacionales

Los *data centers,* o centros de datos, son aquellas instalaciones en las que se encuentran la infraestructura de telecomunicaciones, la infraestructura de servidores, la de refrigeración, protección anti-fuego y energía, en las que se consideran tanto la redundancia como la resiliencia.

En 1993 *Uptime Institute*, con sede en Reino Unido, creó un sistema de clasificación para centros de datos, mismo que se usa para la certificación empresarial en la industria. El sistema de clasificación se conoce como Tier de cuatro niveles y el criterio que se empleó fue analizar la disponibilidad global del centro de datos; de tal manera que Tier I indica una disponibilidad del 98.9%, Tier II indica una disponibilidad del 99%, Tier III indica disponibilidad del 99.9% y, finalmente, el Tier IV una disponibilidad del 99.99%. *Uptime Institute* otorga certificaciones en 71 países para el diseño y las instalaciones construidas de centros de datos **[34]**.

En 1999 la *International Computer Room Experts Association* (ICREA), con sede en México, creó su propio estándar para certificar la operación de centros de datos, para ello utilizó un sistema de clasificación de cinco niveles, que fue denominando ICREA. El nivel I se usa para una disponibilidad de 98.9%, el nivel II para disponibilidad del 99%, el nivel III para disponibilidad del 99.9%, el nivel IV para la disponibilidad del 99.99% y el nivel V para una disponibilidad del 99.999%. lCREA actualiza su estándar cada 2 años, de modo que el estándar actualizado es el ICREA-STD-131-2021 **[35].**

Ante tal competencia, *Uptime Institute* actualmente ofrece certificaciones sobre operatividad de los centros de datos. La más reciente de sus certificaciones incluye centros de datos modulares y prefabricados.

En la estandarización de data centers en México se aplican principalmente los estándares creados por UPTIME (institución de origen británico) e ICREA (institución de origen mexicano) las cuales se abordarán brevemente. Los data centers conforman la infraestructura de tecnologías de frontera, necesaria para la economía digital del presente y futuro, básicamente considerando la "Big Data", la cual excede las capacidades de procesamiento de los sistemas de gestión de bases de datos relacionales y requiere enormes sistemas de almacenamiento. Por ejemplo, se estima que para 2007 la humanidad había almacenado globalmente cerca de 20 exabytes ($20x10^{18}$ Bytes), para 2012 aproximadamente 2.8 zettabytes ($20x10^{21}$ Bytes) y para 2020, 140 zettabytes.

La figura 8 muestra el tráfico en la Internet comercial en todo el mundo, de modo que actualmente nos encontramos en la era Zettabyte (ZB).

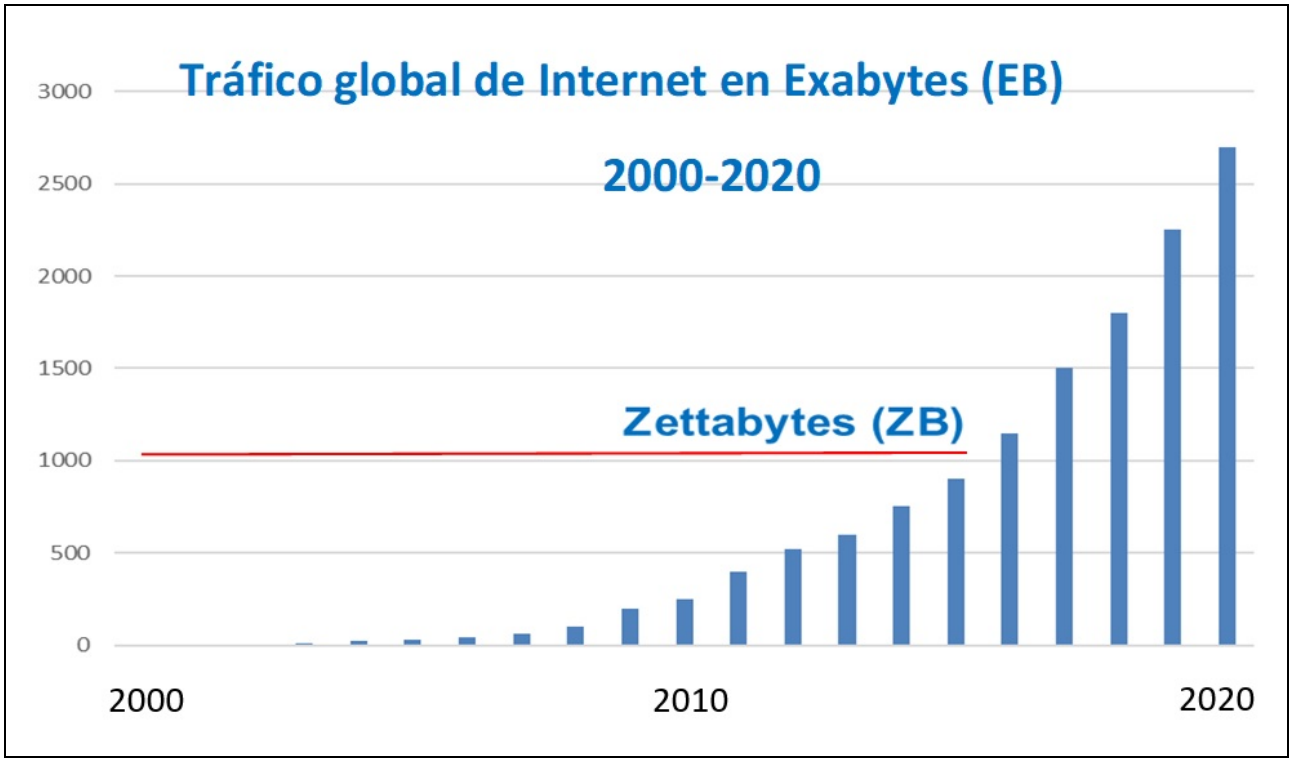


Fig. V.7. Tráfico global de Internet comercial en el siglo XXI.

V.2.1 ICREA

La *International Computer Room Experts Association* (ICREA) se creó en 1999 y certifica desde 2003, a *data centers* en 10 países con relación a documentos de diseño, instalaciones construidas y la sostenibilidad operacional. Para sus certificaciones, ICREA actualmente utiliza los niveles del I al VI, de acuerdo con la norma ICREA-std-131-2021. La norma genera un conjunto de recomendaciones y mejores prácticas, de modo que cada uno de sus niveles describan niveles crecientes de confiabilidad y seguridad. La norma cubre toda industria, incluso aquellas de misión o infraestructuras críticas.

Las áreas que deben observarse para hacer las evaluaciones para las certificaciones y las normas internacionales que deben cumplir se muestra en la tabla V.2, donde se indican 7 de 8, ya que el área o proyecto de **ciberseguridad** no cuenta con normas nacionales ni internacionales **[35].**

	Áreas / proyectos	Normas internacionales
	Instalaciones eléctricas Puesta a tierra, acometidas y alimentadores eléctricos de CA, circuitos derivados de energía ininterrumpible, protecciones, canalizaciones, tableros eléctricos, sistemas de medición y monitoreo, grupos electrógenos de energía de respaldo, transformadores, UPS, SPD, baterías, acometidas y subestaciones, instalaciones de CD.	NFPA 70E/780, IEEE 1100/1106/1188/1187/1584, IEC 6235/88528, ASTM F1506, NESC, ISO 45001, CSA Z462, NRF-254, NEMA, UL 1283/1449
	Climatización Componentes - CRAC, CRAH, CAHU, CCCU-ventilación, limpieza del aire, temperatura y humedad, rejillas difusoras y de retorno, exclusas de acceso y compuertas para aire.	ASHRAE 34/90.1/127/TC9.9, ANSI/ISA-71.04, ISO 817
	Instalaciones de seguridad física Control de acceso, detección de fuego, extinción de fuego, barreras de protección, medios de almacenamiento de datos, protección de medios de respaldo, CCTV, personal en la zona oscura, equipo de seguridad, comunicaciones de seguridad, mantenimiento.	NFPA 10/13/15/20/72/76/80/251/2001, EN54-20, NEMA 4/250, UL 1479, ASTM E814, BS476-20
	Comunicaciones Cableado estructurado, canalizaciones y espacios para comunicaciones, sistema de administración.	ANSI/TIA568/862-B, ISO/IEC 11801-1/14763, IEEE 802.3, IEC 60754/61034/60332/61754, TIA-604, NMX-I-14763-2-NYCE-2017, UL2024, INCITS 479/533/543/2221
	Ámbito Obra civil, piso técnico elevado, EMC Y EMI, ambiente industrial, localización de equipos TIC, estructura del inmueble, compartimentación, sistemas de iluminación, CDP de respaldo.	ISO 8528-10/ R-3744, NFPA75/101/110/704, EN1047-2, NBR11515, NBR15247, BS1047-2
	Gobernabilidad Gestión de riesgos, administración y licenciamiento, operación de data center, mantenimiento del *data center*, gestión de la disponibilidad y continuidad del negocio, pruebas y comisionamiento, gestión del CapEx, gestión del OpEx, gestión de la adquisición y suministro, herramientas y automatización, gestión de proyectos, sistemas de gestión de los data centers, certificaciones, cumplimiento corporativo.	ISO 9001/ 14001/ 20000/ 22301/ 27001/ 31000/ 37301/ 38500/ 45001/ 50001
	Sustentabilidad Gobierno, administración y planeación, sistemas eléctricos, sistemas de climatización, ámbito y arquitectura, equipos de TI, métricas y monitoreo, eficiencia energética y mejores prácticas.	ISO14000 / 50001 / 55000, ITIL, Green Grid Wp349, CoE 2021 v 11.1.0, TP-1-199, DOE2016

Tabla V.2. Proyectos y normas internacionales que cumple el ICREA Std-131-2021.

Se considera que las siglas de las instituciones internacionales que generan las normas son conocidas por el lector con perfil de ingeniería a quien se dedica esta obra. A continuación, se resumen las características generales que se dan a cada nivel de certificación por parte de ICREA.

Nivel I: Quality Assurance Data Center (QADC)

La infraestructura incluye un espacio dedicado para los sistemas de TI (Tecnologías de la información) generalmente llamado *Site o Room*; cuenta con sistemas de respaldo de energía (*Uninterruptible Power Supply* - UPS), un equipo para enfriamiento y un generador de energía, por lo general de diésel, para enfrentar los cortes energéticos de electricidad. En este nivel se espera una disponibilidad anual del 95%, de allí que se denomine Nivel I por un nueve.

Nivel II: World Class QADC (WCQA)

La infraestructura cuenta con las características de Nivel I y además con redundancia para los componentes críticos en energía (UPS y generador), y en enfriamiento, los que conocemos cómo *chillers* o bombas; para presentar cierta tolerancia a fallos. En este nivel se espera una disponibilidad anual del 99%; de allí que se denomine Nivel II por los dos nueves, que definen su eficacia.

Nivel III: Safety WCQADC (SWCQA)

La infraestructura cuenta con las características de Nivel II y además con una ruta redundante para la entrega de energía eléctrica (segunda toma); así como redundancia en el enfriamiento, con la finalidad de que (pese a que se desconecte el sistema principal de energía y enfriamiento para realizar maniobras de mantenimiento), el sistema pueda operar sin impactos sobre la operación de TI. En este nivel se espera una disponibilidad anual del 99.9%; de allí que se denomine nivel III por los 3 nueves que definen su eficacia.

Nivel IV: High Security WCQADC(HS-WCQA)

La infraestructura cuenta con las características de Nivel III y además cada equipo posee redundancia, de modo que, si hubiera una falla de equipos individuales o interrupciones en el suministro de energía eléctrica, estos eventos no detengan la operación del sistema de TI; es decir, deben ser tolerantes a fallos. En este nivel se espera una disponibilidad anual del 99.99%, de allí que se denomine Nivel IV, por los 4 nueves que reflejan su desempeño.

Nivel V: High Security High Available WCQADC(HSHA-WCQA)

La infraestructura cuenta con las características de Nivel IV y además, para el caso del sistema eléctrico, debe tener una configuración con redundancia sin puntos únicos de falla (PUF), que también permita dar mantenimiento sin suspender la operación y siendo tolerante a fallas, tal que la acometida tenga redundancia 2N y el UPS igualmente con doble banco de baterías en cada UPS. En UPS mayores a 100kVA, las baterías se deben colocar en cuartos independientes, de modo que estén separadas y compartimentadas, con un rango de temperatura entre 18ºC y 27ºC. Los bancos de baterías deben soportar plena carga a 100%, con redundancia N+1, y las baterías deben probarse cada 3 meses, es decir, 4 veces al año. La calidad de la energía se debe medir de manera continua y automática. Los tanques de combustible deben garantizar un trabajo continuo de mínimo 72 horas. Cada equipo cuenta con redundancia, de modo que, si existiera una falla en los equipos individuales o interrupciones en el suministro de energía eléctrica, estos eventos no detengan la operación del sistema de TI. En este nivel se espera una disponibilidad anual del 99.999%, de allí que se denomine Nivel V por los 5 nueves, que reflejan su desempeño superior.

Es necesario que los **data centers de redundancia**, estén físicamente a distancias mínimas de 7 Km y en el caso de los **planes de recuperación ante desastres** (*Disaster Recovery Plan* - DRP) los *data centers* deben estar a mínimo 250 Km.

Nivel VI: Redundant High Available Net (RHA-WCQADC)

Aquí ya no se habla de *data centers* individuales, sino de una red o arreglo de por lo menos 3 data centers de Nivel III, certificado independientemente, con una sincronización entre ellos que permita una disponibilidad anual del 99.9999%, de allí que se denomine Nivel VI, por los 6 nueves de su eficiencia, que aún se sigue perfeccionando. Los *data centers* deben estar distanciados entre ellos, como mínimo, a 50 Km.

V.3 Métricas para *Data Centers*

Para *data centers,* cada vez se agregan más métricas en las que se busca priorizar la eficiencia, principalmente la eficiencia energética, buscando los máximos ahorros energéticos que permitan una reducción de gastos significativa. Entre ellas, las cuatro métricas más populares serán abordadas brevemente **[36, 37]**.

- Data Center Infrastructure Efficiency (**DCIE**)

$$DCIE = (1 / PUE) \times 100\% \quad \text{[Ec. V.1]}$$

- Power Usage Effectiveness (**PUE**)

$$PUE = \text{Energía anual total consumida por las instalaciones} / ETI \quad \text{[Ec. V.2]}$$

- Water Usage Effectiveness (**WUE**)

$$WUE = \text{Uso anual de agua (L)} / ETI\ [L/(kWh)] \quad \text{[Ec. V.3]}$$

- Carbon Usage Effectiveness (**CUE**)

$$CUE = \text{Emisión de CO2 total} / ETI\ [kg\ CO_2eq\ /(kWh)] \quad \text{[Ec. V.4]}$$

Donde

ETI = Energía anual del equipo de TI (kWh)

Tanto las métricas WUE como CUE deben mantenerse lo más bajas posible, y PUE debe tender a 1 para ser más eficiente.

V.4 Identificación de número de sistema autónomo de proveedor

En la figura V.8 se muestra una captura de la medición de velocidades de bajada y subida que ofrece un proveedor de internet para un usuario final. Observe los parámetros de latencia y jitter, pero principalmente, note que el número de sistema autónomo (*Autonomous System Number*-ASN) asignado al proveedor "Totalplay" es AS17072.

Debe considerar que, al ser Totalplay uno de los ISP, de tamaño considerable con cobertura nacional, este tiene asignados varios ASN en México. Cada compañía ISP, en función de su tamaño y cobertura, tiene uno o varios ASN. Como actividad, puede usar la siguiente liga para realizar su propia prueba https://selectra.mx/internet-casa/speedtest

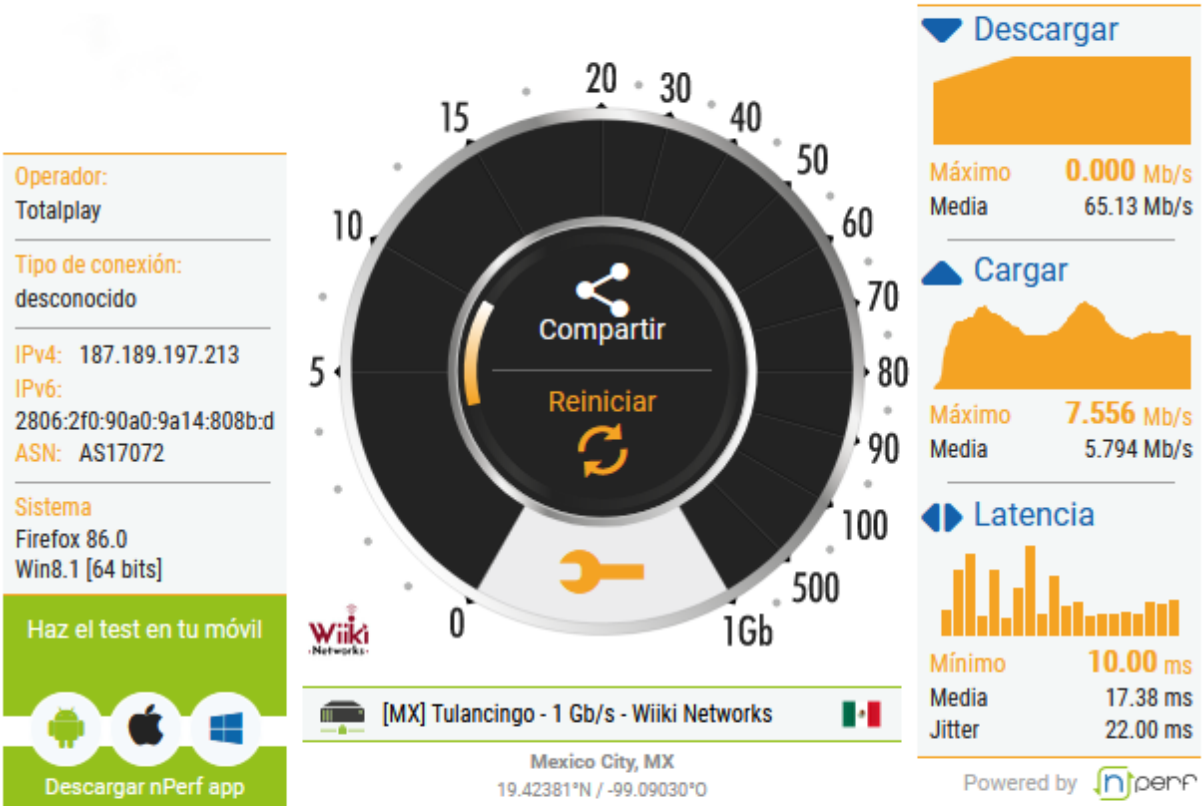


Fig. V.8. Identificación del número de sistema autónomo de un proveedor de internet a usuario final general.

V.5 PRÁCTICA 6: Infraestructura

El objetivo de esta práctica es que usted identifique todos los elementos claves de la infraestructura de redes.

Actividad 1: Simule la infraestructura de una red MAN, la cual interconecta 5 redes LAN, correspondientes a 5 campus universitarios, los cuales se interconectan bajo una topología de anillo (interconectada por fibra óptica), como se indica en la figura V.6. Considere un *router* por cada LAN y un *router* tipo *core* en cada MDF. Muestre explícitamente las redes y coloque todos los switches indicados en la tabla V.1 y, al menos, 2 host por cada switch.

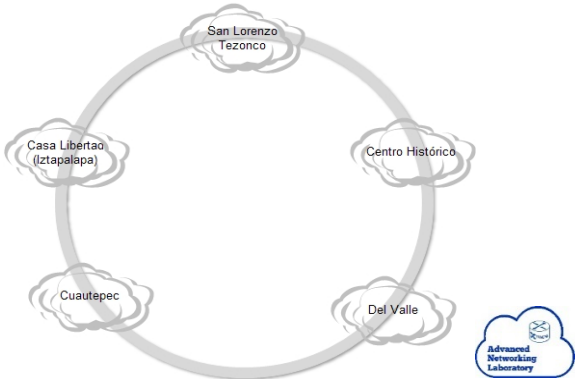


Fig. V.6. Topología para la red MAN que une los distintos campus de la UACM.

Actividad 3. Con la finalidad de tener una mejor idea acerca de los data centers, deben consultar el siguiente video: *Green Mountain Data Center High-Resolution* https://www.youtube.com/watch?v=EaeokJECyIs

Actividad 3. Obtenga las referencias [38] y [39] que corresponden a los *white papers* para el estándar para *data centers* de la TIA y el modelo de madurez de capacidades para *data centers* de The Green Grid, asegúrese de entenderlos y poder explicarlos **[38, 39]**.

Actividad 4 (Opcional): De ser posible, realice una visita a instalaciones MDF e IDF de la red en su institución, así como la infraestructura de red para identificar *switches*, *routers*, servidores, SAN, sistemas eléctricos y de refrigeración y, todavía mejor, si puede, visite un centro de datos.

V.6 Capacidad para manejar las tecnologías de frontera

Actualmente se considera que las tecnologías de frontera son once: Inteligencia artificial, Internet de las cosas (*Internet of Things* - IoT), datos masivos (Big Data), cadena de bloques (*Blockchain)*, robótica, Drones, impresión 3D, comunicación 5G, edición genética, Nanotecnología y tecnologías fotovoltaicas solares. Entonces, surge la pregunta: ¿Qué tanto los países, instituciones y personas están preparadas para la creación, desarrollo y uso de las tecnologías de frontera?

Con la finalidad de medir las capacidades para el manejo de las tecnologías de frontera, la ONU ha generado el "Índice de preparación para las tecnologías de frontera (*Readiness For Frontier Technologies Index*)'. Para obtener tal índice, se consideran 5 bloques o grupos de indicadores **[40]**:

A) Despliegue de las TICs

Este indicador mide el nivel de la infraestructura y es vital, ya que el uso, adopción y adaptación de las tecnologías de frontera necesitan infraestructura que sea suficiente en cantidad y calidad; aquí es donde entran los data centers y la conectividad a la internet.

B) Habilidades

Para el uso, adopción y adaptación a las tecnologías de frontera, se requiere gente con las habilidades que sean relevantes, tanto aquellas que se adquieran a través de la educación académica (midiendo los años de preparación), como aquellas que se adquieren en el ámbito laboral, mediante el entrenamiento práctico o el aprendizaje, lo que se adquiere haciendo una actividad relacionada con las tecnologías de frontera (midiendo la cantidad de administradores, técnicos y profesionales asociados a empleos de alta especialización). Las métricas están definidas por la *International Standard Classification of Occupations* (ISCO), sin embargo, la ONU hace énfasis en que los migrantes considerados altamente calificados, cuyo origen está en los países en vías de desarrollo pueden tener un nivel de habilidades inferior al oficialmente registrado en los países desarrollados, y la experiencia nos confirma que existe mucha evidencia de ello, tanto a nivel académico como en la industria.

C) Actividad de investigación y desarrollo

Este indicador es importante por cuanto se produce tecnología de frontera, pero también cuando se adopta y adapta localmente una tecnología, para ello se consideran dos métricas: "el número de artículos en tecnología de frontera publicados", en la base de datos de SCOPUS, donde se analizan 234 países, y el "número de patentes registradas anualmente en tecnologías de frontera", en la base de datos PatSeer entre 234 países. De ambas bases de datos se usó la estadística desde 1996 a 2018, ya que las bases de datos son más confiables desde 1996 en adelante. Se hace referencia también

al hecho de que en los países en vías de desarrollo se hace investigación y desarrollo de manera informal. La experiencia nos confirma también que existe mucha evidencia de ello, principalmente en el ámbito académico; incluso algunos investigadores lo hacemos más como un pasatiempo o afición, con nuestros propios recursos, que como una investigación planeada y financiada por alguna institución. La tabla V.3 muestra el número de publicaciones en SCOPUS y de patentes en PatSeer desde 1996 a 2018, así como los países que lideran en las once tecnologías de frontera **[40]**.

Tecnologías	Publicaciones	Países líderes	Patentes	Países líderes
Inteligencia artificial	403,596	EUA, China, Reino Unido	116,600	EUA, China, Alemania
Internet of Things - IoT	66,467	China, EUA, India	22,180	China, Corea, EUA
Big data	73,957	China, EUA, India	6,850	China, Corea, EUA.
Blockchain	4,821	China, EUA, Reino Unido	2,975	EUA, Antigua Barbuda, China
Robótica	254,409	EUA, China, Japón	59,535	EUA, Corea, Alemania
Drones	10,979	EUA, China, Reino Unido	10,897	EUA, Corea, Francia
Impresión 3D	17,039	EUA, China, Alemania	13,215	EUA, Corea, Francia
Comunicación 5G	6,828	China, EUA, Reino Unido	4,161	Corea, China, EUA.
Edición genética	12,947	EUA, China, Reino Unido	2,899	EUA, Suiza, China
Nanotecnología	152,359	EUA, China, Alemania	4,293	EUA, China, Rusia
Tecnologías fotovoltaicas solares	10,768	India, EUA, China	20,074	China, Corea EUA

Tabla V.3. Publicaciones y patentes en las 11 tecnologías de frontera.

D) Actividad industrial

Este indicador registra actividades relacionadas con el uso, adopción y adaptación de las tecnologías de frontera. Se hace referencia al hecho de que en países en vías de desarrollo es posible encontrar actividad industrial no registrada debido a cuestiones de informalidad. Para este aspecto se consideran dos casos, uno es el porcentaje de mercancía que se exporta como producto de alta tecnología, con respecto del total, y el otro corresponde a los servicios digitales que se exportan, como porcentaje del total de servicios vendidos. En los registros, sólo hay indicadores para 216 y 186 países respectivamente.

E) Acceso a financiamiento

Este indicador muestra la facilidad de acceder a créditos o financiamientos que permiten acelerar el uso, adopción y adaptación a las tecnologías de frontera, específicamente se mide por el porcentaje del PIB que un país otorga como crédito interno al sector privado. Y es, precisamente en países en vías de desarrollo, donde más pueden invertir las grandes corporaciones de países más desarrollados, principalmente por el tipo de cambio y los incentivos fiscales dados a los inversionistas. Este indicador es importante, porque deja en claro la razón por la que en el ambiente académico existe una baja inversión en investigación y desarrollo que genera pocas patentes nacionales, pues la mayoría de estas son extranjeras y provienen de las grandes corporaciones.

La tabla V.3 muestra el índice de preparación para las tecnologías de frontera para países americanos, considerando los 4 grupos ponderados al 25%: Alto, medio alto, medio bajo y bajo. El índice promedio es de 0.44. De esta manera nueve países latinoamericanos están en el nivel de media alta, el resto en media baja y baja [40].

País	Posición global	Índice	Grupo
EUA	1	1	Alto
Canadá	14	0.89	Alto
Brasil	41	0.61	Media-alta
Chile	49	0.57	Media-alta
México	**57**	**0.54**	**Media-alta**
Costa Rica	61	0.51	Media-alta
Argentina	65	0.49	Media-alta
Panamá	67	0.49	Media-alta
Uruguay	68	0.47	Media-alta
Trinidad y Tobago	75	0.45	Media-alta
Colombia	78	0.44	Media-alta

Tabla V.3. Índice para países de América de 158 países en el mundo.

CAPÍTULO VI: GESTIÓN DE RED

Con la evolución de los protocolos de gestión, desde aproximadamente 2005, a nivel comercial y no sólo militarmente, los ISP pueden apagar o encender cajeros automáticos, cámaras o cualquier equipo electrónico conectado a la Internet de manera remota. En esta década será posible apagar no solo tarjetas de crédito o débito digitales, sino las monedas digitales como el "yuan chain coin" *(e-CNY)* - la primera moneda digital liberada por el gobierno chino, en febrero de 2022 - incluso los distintos tipos de dólar o las monedas digitales que se vayan generando por parte de los bancos centrales.

De manera recurrente, en el ámbito de las TICS, hablamos de la pirámide de la información, la cual se divide en datos, información, conocimiento y sabiduría. Cada una de las cuatro áreas apiladas se relacionan con su propia base de datos, base de información, base de conocimiento y base de sabiduría, respectivamente, recordando que partimos de los datos simples, los cuales tienen un único valor, y los datos estructurados, que tienen varios componentes. La figura VI.1 muestra la pirámide de la información, donde el ancho indica cantidad y la altura implica calidad.

La gestión de una red implica no sólo tener una base de datos, sino una base de información, a la cual llamamos Base de Información de Gestión (*Management Information Base* - MIB). Para ello, se usa un árbol, también llamado árbol de Internet. Un árbol es una estructura de datos, la cual organiza a la información de manera jerárquica.

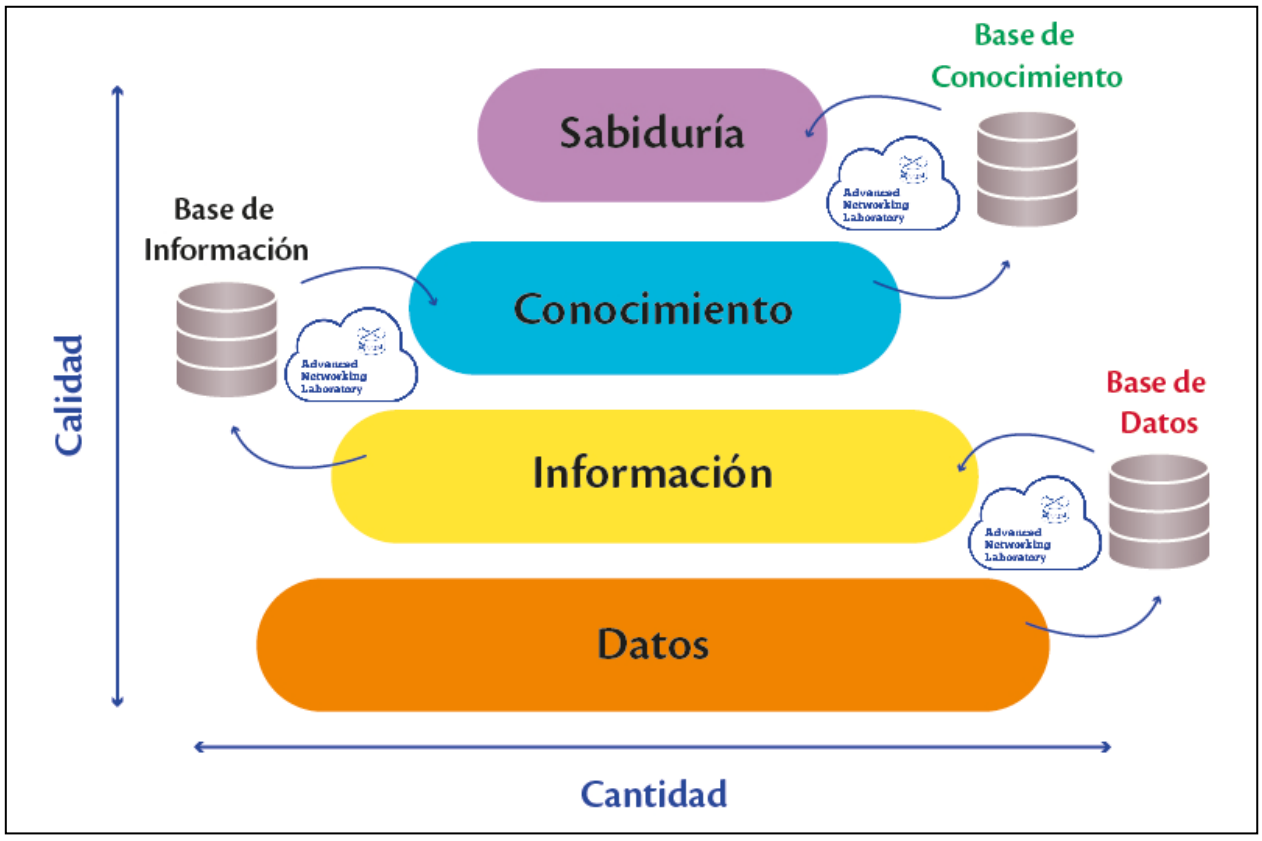


Fig. VI.1 Pirámide de la información y el conocimiento.

Con base en esta pirámide fue que la ONU popularizó el término sociedad de la información y el conocimiento.

VI.1 La gestión de una red

La gestión de toda red debe cubrir básicamente 4 actividades: el monitoreo de la red (*Monitoring*), la configuración de equipos de comunicaciones (*configuring*), la actualización del software (*updating*) y la resolución de problemas (*troubleshooting*). Todo administrador de red, en cualesquiera compañía, empresa o campus universitario que gestione una red, realizará estas 4 actividades como mínimo. En una red de backbone se pueden administrar cientos o miles de elementos. Si la complejidad fuera baja y sólo contáramos con datos, se requeriría de una base de datos para almacenarlos. Sin embargo, la complejidad de cada elemento de red es tal, que por cada uno de ellos, se cuenta con bastante información, por lo que se requiere una base de información (*Information Base* - IB) para la gestión, a la cual llamamos *Management Information Base* (MIB).

Los 3 elementos necesarios para gestionar una red

A) **Un sistema de gestión de red** (*Network Management System*-NMS), es un software que se instala en un host y servirá como consulta desde donde se monitorea, configura actualiza o se resuelven problemas. Por lo general, a ese software se le conoce como MIB *browser,* ya que requiere de una MIB para interactuar con los elementos de una red.

B) **Equipos de comunicaciones** por gestionar, ya sean *routers* o *switches* u otros equipos, los cuales cuentan con elementos que se pueden monitorear o controlar, tales como fuentes de alimentación, ventiladores, sensores de temperatura, interfaces, memorias *flash*, etc.

C) **Agentes de software** que hacen el puente entre el NMS y cada equipo a gestionar, de tal modo que un agente se instala, activa o habilita en cada equipo por gestionar. Un agente permite tener comunicación con un host o un *router*, de tal modo que el equipo sea administrado desde una estación de gestión. Entonces, el MNS interactuará directamente con el agente y el agente trabajará con los elementos del equipo a gestionar, para lo cual este debe acceder constantemente a la base de información para la gestión (MIB). Para realizar ese trabajo los agentes deben usar un protocolo de gestión; el más popular es el "protocolo de gestión de red simple" (*Simple Network Management Protocol* - SNMP). La evolución del SNMP se resume en la tabla VI.1. En el caso de los estándares de internet se indican las tres fases típicas **[41-46]**.

Proposed Standard	Draft Standard	Internet Standard
SNMP v1		
RFC 1067-1988, RFC 1098-1989 RFC 1157-1990 (Histórico)		
SNMP v2		
RFC 1448-1993	RFC 1905-1996	**RFC 3416-2002**

Tabla VI.1 Evolución del SNMP

¿Qué es la MIB y cuál es la estructura de la información?

La MIB es una estructura de información que describe a un equipo como una lista de elementos, a los que ve como objetos, para lo cual debe asignar un identificador de objeto (*Object Identifier* - OID). Para ello un OID se representa como una secuencia de números enteros separados por puntos. Cada entero representa un nodo en una estructura de árbol, la cual ayuda a que se simplifique la búsqueda de información. A este árbol se le conoce como el "árbol de Internet", el cual se muestra en la figura VI.2. Observe que el OID 1.3.6.1 corresponde a una rama que llega a Internet (1-ISO.3-ORG.6-DOD.1-Internet), el cual consta de 6 subárboles, que se describen en la tabla VI.2

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

Tabla VI.2 Los 6 subdirectorios del árbol de Internet.

En el árbol de Internet, podemos identificar los nodos generados de manera genérica, vía el *mgmt* (OID=1.3.6.1.2), pero también aquel del protocolo *snmpv2* (OID=1.3.6.1.6); pero de gran importancia son aquellos correspondientes a los OID específicos de las compañías que fabrican *switches y routers*, indicados bajo *private* (OID=1.3.6.1.4). Por ejemplo, los OID que genera la compañía CISCO *Systems*, quedan como objetos que componen el árbol a partir del OID 1.3.6.1.4.1.9, como se indica en la figura VI.2. Hasta este punto, los OID son abstracciones, pero los elementos específicos que pueden manejarse y tener una relación con el mundo físico u objetos reales se observan en el siguiente ejemplo:

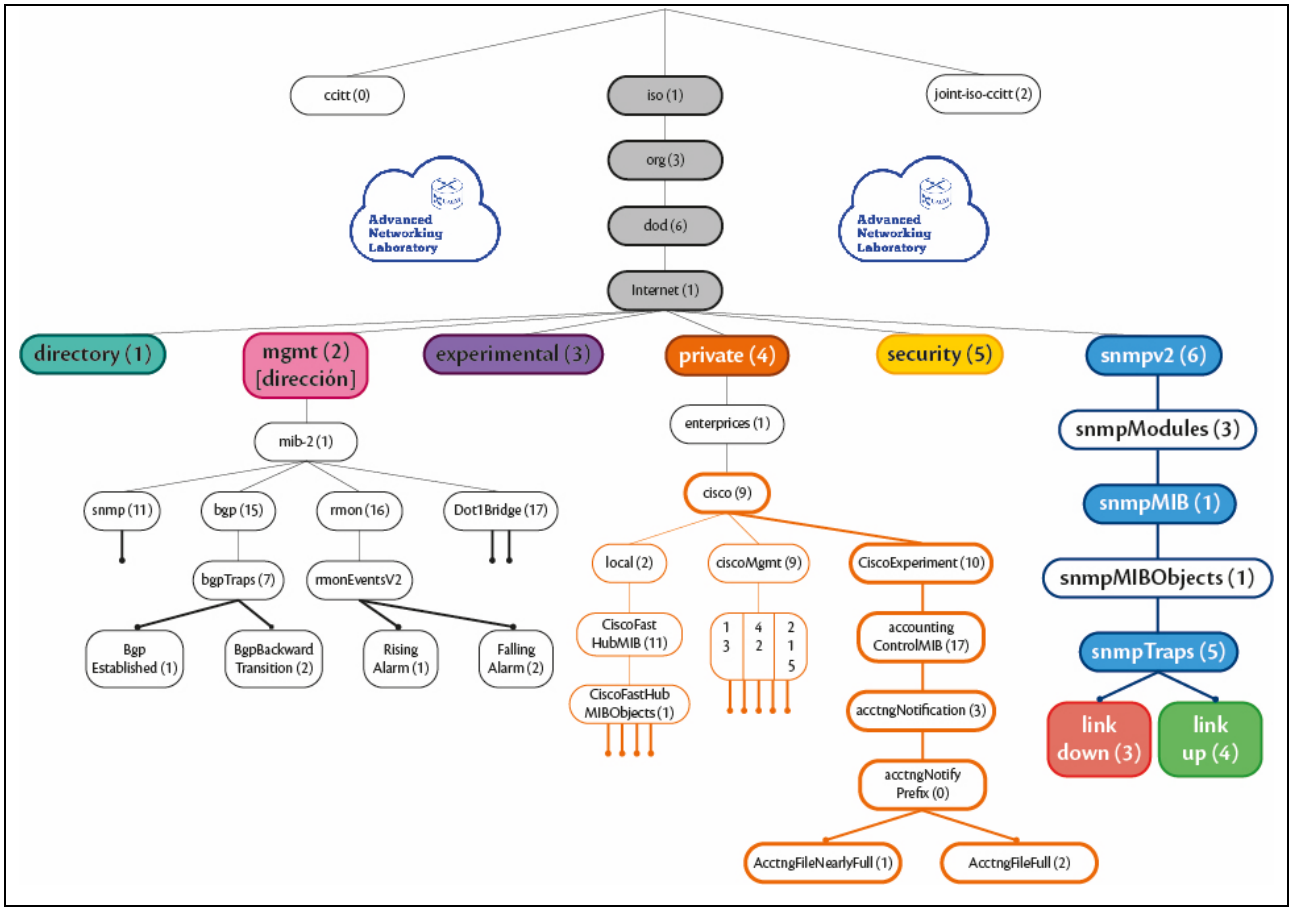


Fig. VI.2 Los OID como nodos dentro del árbol de internet.

¿Cómo detectamos que un enlace dentro de una red se ha desconectado?

De inicio, decimos que un enlace se ha caído y, para esto, concentrémonos en el OID 1.3.6.1.6.3.1.1.5.3, de modo que este elemento se conoce como un *trap* de LINKDOWN; es decir, es un tipo de alarma que indica que un enlace se ha desconectado o deshabilitado o caído. Este tipo de alarma se genera desde la tarjeta de red y se detecta a través del agente de SNMP, el cual notifica al NMS, ubicado en algún host, desde el que se monitorea a la red. De manera similar, podemos monitorear a través de sensores, la temperatura de un chip, el estado de un ventilador, el estado de una fuente de alimentación, el estado de una interfaz de comunicación serial o paralela u otra, el estado físico o administrativo de un enlace.

Los OID como variables

Cada OID se almacena en *registros,* como variables, que pueden ser solamente consultadas o leídas (variable con permiso de lectura o *read*); o leídas y escritas (variable con permiso de lectura y escritura *read-write*). En general cada objeto a gestionar cuenta con, al menos, 5 elementos:

nombre, OID, sintaxis, modo de acceso a la variable y descripción. En la figura VI.3 observamos, en el simulador *Cisco Packet Tracer,* un objeto al que llamamos *sysName*, el cual corresponde al nombre del sistema o equipo a gestionar. Su OID corresponde a 1.3.6.1.2.1.1.5., este nombre del equipo se guarda, en una variable del tipo *octetString,* y tiene permisos de lectura y escritura.

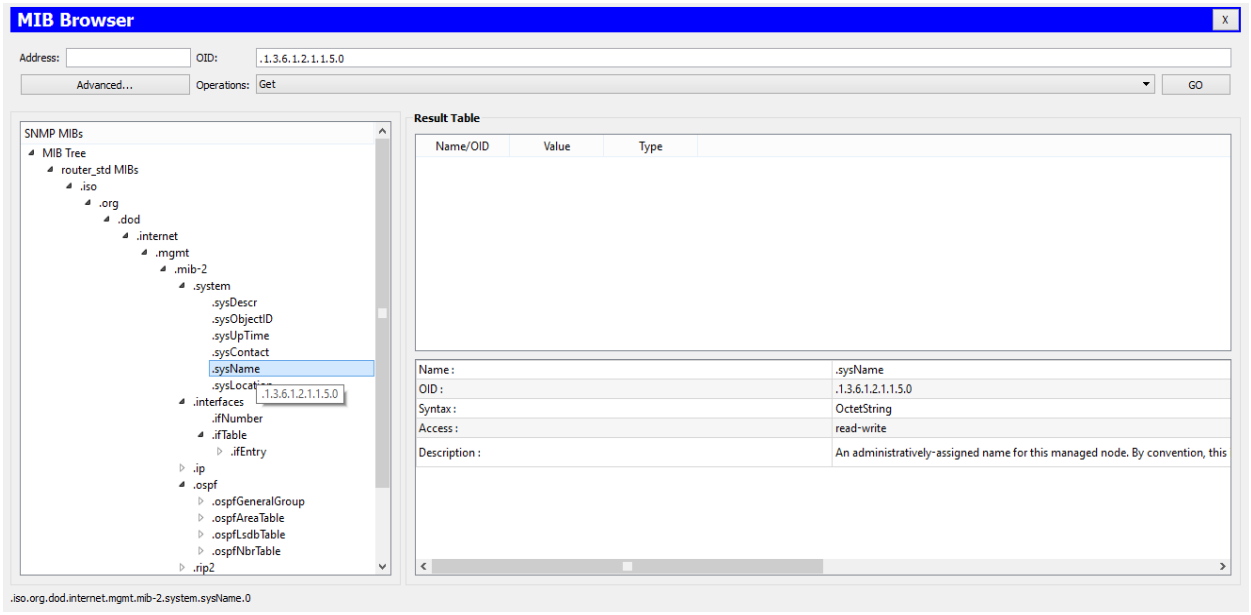


Fig. VI.3 Componentes del objeto *sysName* a gestionar.

Existen otros objetos que sólo tienen permiso de lectura, por razones obvias, por ejemplo, el número de interfaces deberá ser sólo de lectura, para evitar que lógicamente se pueda indicar un determinado número de interfaces que no corresponda al número real de interfaces. En la misma figura VI.3, es posible observar, en el área SNMP MIBs, al objeto *ifNumber,* el cual indica el número de interfaces con las que cuenta, por ejemplo, un *router.* La variable sólo tiene permiso de lectura; es decir, el agente identifica el número de interfaces y lo reporta al NMS; en este caso se emplea la operación GET.

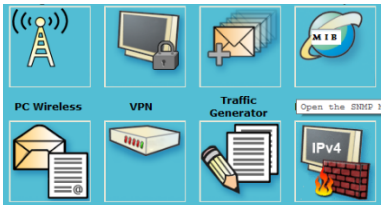
VI.2 SNMP: Configuración de agentes

SNMP es un protocolo que maneja sus mensajes bajo dos métodos diferentes: *Polling* (encuesta) y *Traps* (trampas). En el primer caso, se hacen consultas remotas de manera síncrona, ya sea de manera activa o bajo demanda desde la estación de gestión; mientras que los *traps* son mensajes asíncronos que se disparan a manera de alarmas. La configuración de un agente SNMP se realiza en un *router,* como se indica en la figura VI.4 [47].

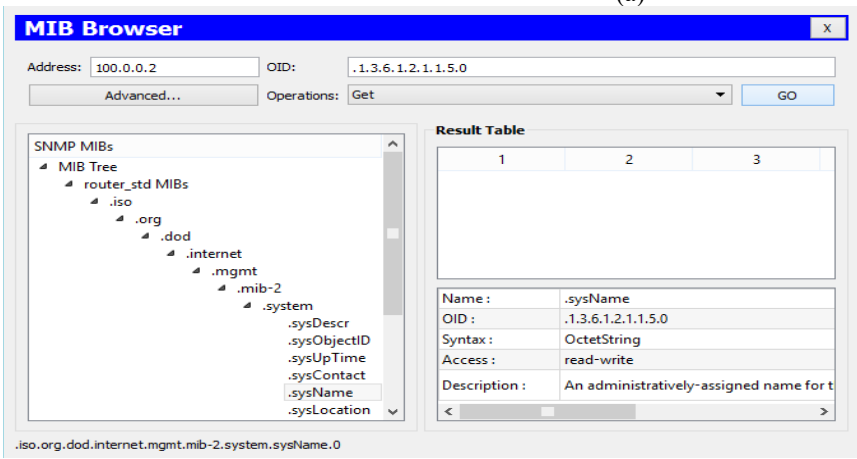
```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#snmp-server community ADVNETLAB rw
%SNMP-5-WARMSTART: SNMP agent on host Router2 is undergoing a
warm start
Router2(config)#exit
```

Fig. VI.4 Configuración del agente SNMP en un *router*.

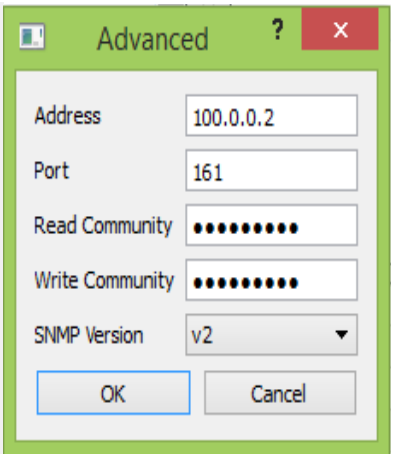
Posteriormente podemos usar un MIB browser, como se indica en la figura VI.5a, para el caso del simulador PKT, y entonces se configuran en el NMS las mismas características que fueron configuradas en el *router*, tales como la versión del SNMP, su comunidad de lectura y escritura, como puede observarse en las figuras VI.5b y VI.5c.



(a)



(b)



(c)

Fig. VI.5 Configuración de agentes en el NMS.

Como caso práctico, la figura VI.6 muestra una interfaz para configurar un *router* Juniper E320.

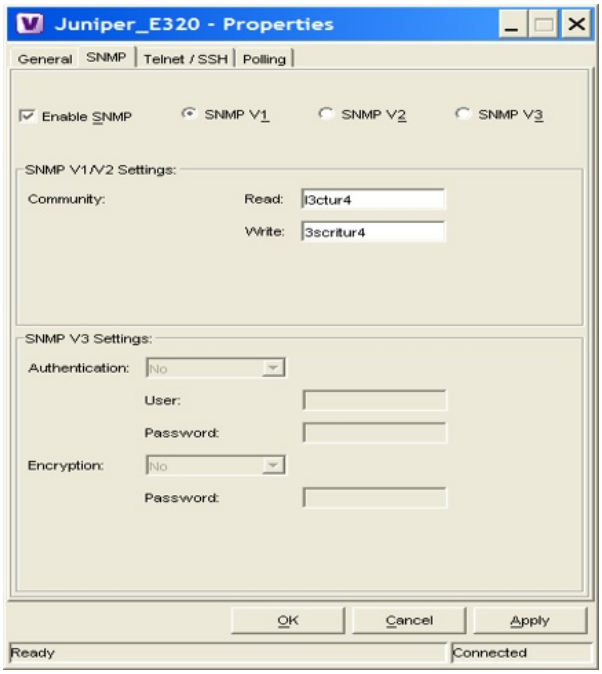


Fig. VI.6 Interfaz gráfica para la configuración SNMP en un *router* Juniper.

Observe la versión y las comunidades de lectura y escritura. Sólo cuando se elige la versión 3 es posible configurar el tipo de autenticación y de encriptación. Por su parte, la figura VI.7 muestra la configuración del agente de un *router* Juniper; observe el estado del agente como activado.

Fig. VI.7 Interfaz gráfica que muestra los generales de un agente SNMP en un *router* Juniper.

VI.3 SNMP: Comunicación entre un agente y el NMS

La figura VI.8 muestra cómo se detectan paquetes SNMP, que salen del *router* 2.

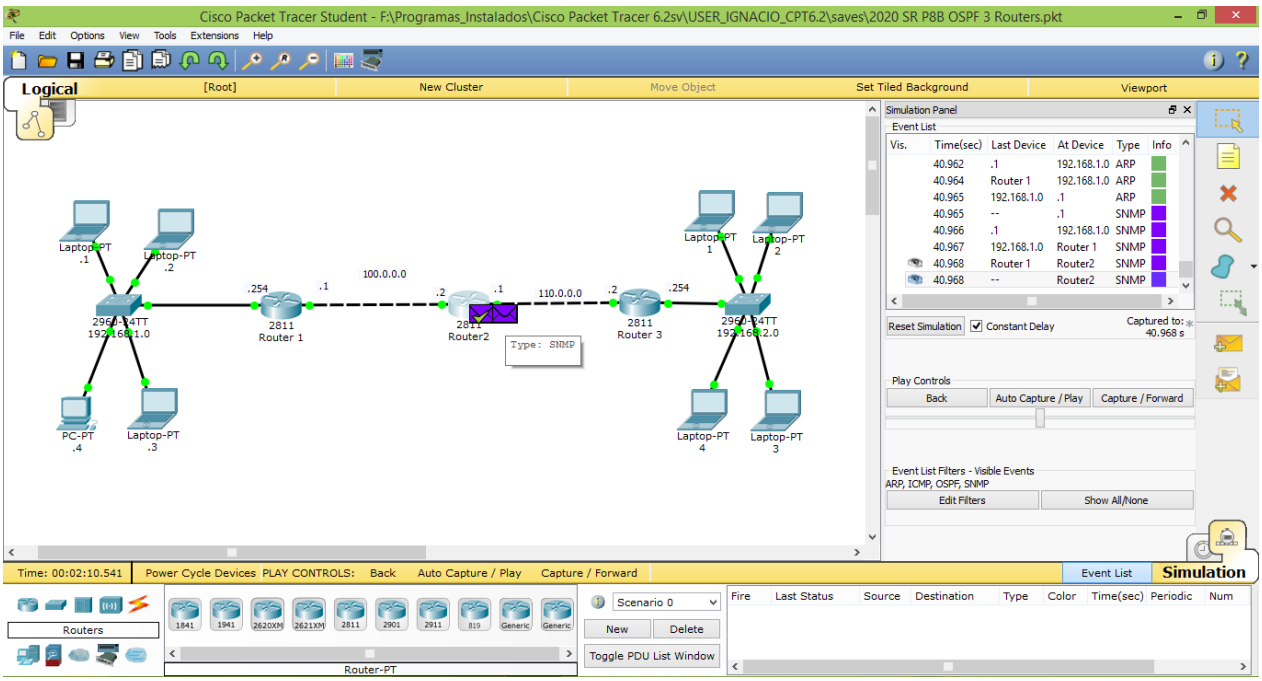


Fig. VI.8 Topología de una red e identificación de los paquetes SNMP.

Un segmento SNMP, correspondiente para SNMPv1 o SNMPv2, el cual consta de 3 campos: *Version, Community* y SNMP PDU. La tabla VI.3 muestra el segmento; observe cada uno de los 3 campos de modo tal que la estructura del campo SNMP PDU se encuentra sombreada y, a su vez, se divide en 5 campos **[43, 46]**.

0	8	16	24 31
Version			
Community			
PDU Type			
Error status			
Error Index			
PDU Variable Bindings			

Tabla VI.3 Encabezado de paquete SNMP v1 o v2 para IPv4.

Donde

a) *Version*: Indica la versión del protocolo.
b) *Community*: Autentifica el mensaje SNMP.
c) SNMP PDU: Contiene los atributos que determinan la operación a realizar, en donde:

Error Status (ES) puede tener al menos 2 valores, 0 indica que no hay error y 1 el PDU es demasiado largo.

Error Index (EI): Se indica cuando ES es distinto de cero y podría dar información de la variable que ha causado el error.

Variable Bidings: Campo que contiene la información de los parámetros gestionados con sus respectivos valores, codificados por medio del estándar SMI (*Structure Management Information* – Información de gestión de la estructura). Por ejemplo, si se solicita el nombre de un *router*, el contenido de la variable irá en este campo. Los detalles de un paquete SNMP se muestran en la fig. VI.9, de modo que es posible identificar la versión 2 de SNMP y la clave de comunidad que se usa, tanto para lectura como escritura. En el encabezado de la unidad de datos, que usa el protocolo (*Protocol Data Unit*- PDU), se observa el puerto 161, que se aplica en la capa 4 del modelo TCP/IP.

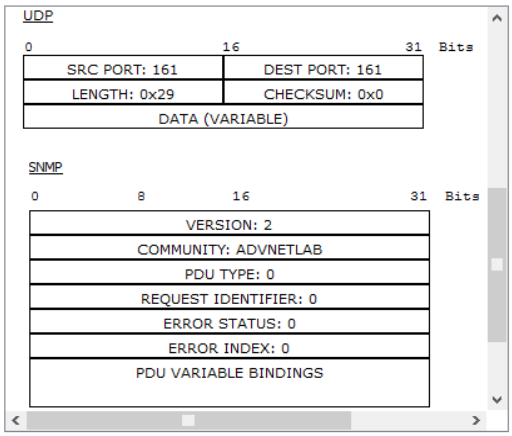


Fig. VI.9 Formato PDU y paquete SNMP.

Y si se desea conocer el nombre del *router*, pero no desde la consola de este *router*, sino desde la computadora que hace las veces del MNS, entonces se usa el software del MIB Browser y se indica la dirección de una de las interfaces que nos conectan con el *router* en cuestión. Por ejemplo, el *router* 2 y se indica, en el MIB browser, que el agente busca al OID correspondiente al nombre del sistema y se obtiene como resultado lo que se muestra en la figura VI.10

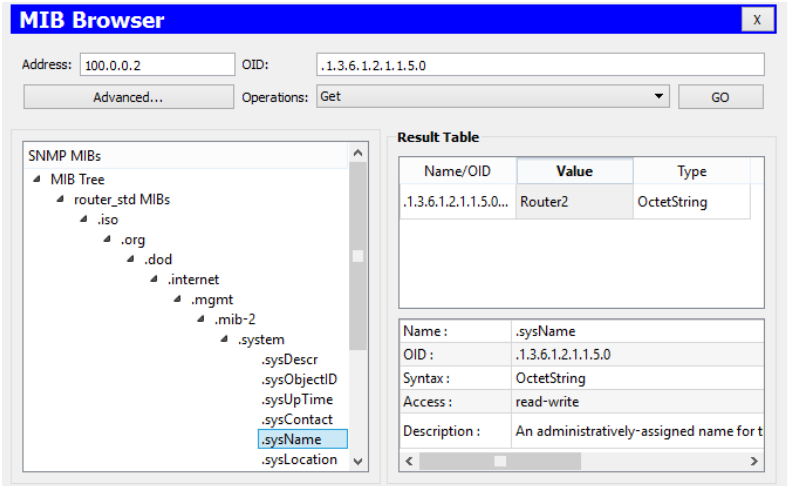


Fig. VI.10 Resultado de la acción de un agente en el NMS.

Y si ahora deseo cambiar el nombre de un *router*, no desde la consola, sino desde la computadora remota donde se ha instalado el software que le hace el NMS, entonces debo ir a la opción de "SNMP SET", en el área de operaciones, e indicar el OID, el tipo de variable a la que corresponde y el nuevo nombre que tendrá esta variable, la cual dará el nuevo nombre al *router*, como se indica en la figura VI.11.

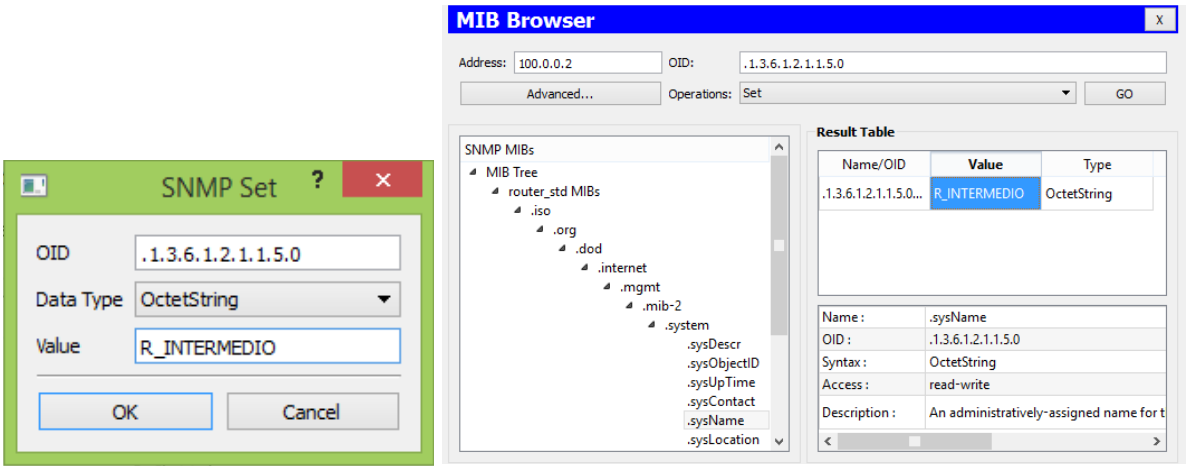


Fig. VI.11 Cambio del nombre de un *router* vía NMS.

Otra operación de utilidad en la gestión de redes es la obtención de las direcciones IP como tablas. En este caso, se usa la operación "GETBULK", para poder traer toda la tabla de direcciones IP, ya que no se traerá una sola variable, sino un conjunto de variables, como se muestra en la figura V1.12, en la que se observan los estados previos al resultado y el resultado de la operación.

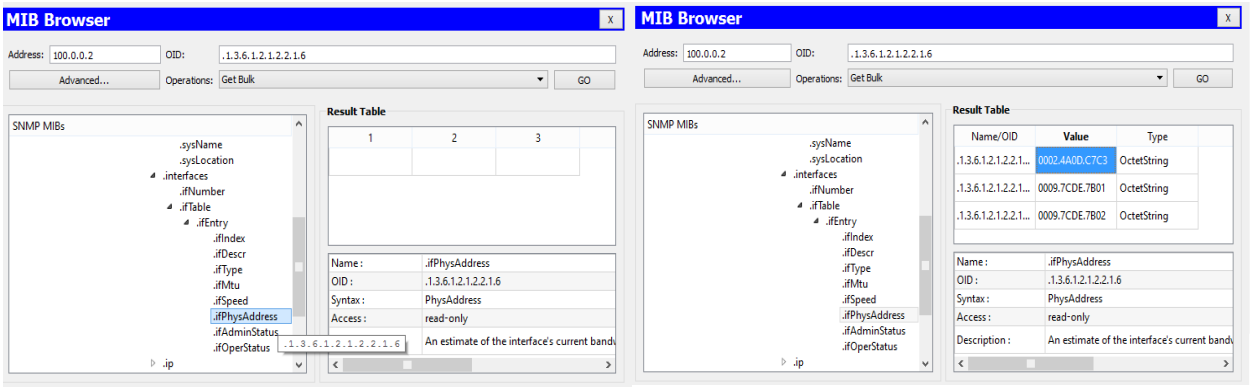


Fig. VI.12 Obtención de las tablas de direcciones vía NMS.

Una de las acciones más recurrentes realizadas desde el NMS es la obtención de las tablas de enrutamiento. En este caso, la figura VI.13, muestra la respuesta a la petición de la tabla de enrutamiento para el *router* 2 y, en la figura VI.14, se aprecia cómo la misma se corrobora al solicitar la tabla de enrutamiento vía el IOS del propio *router* en la interfaz del CLI.

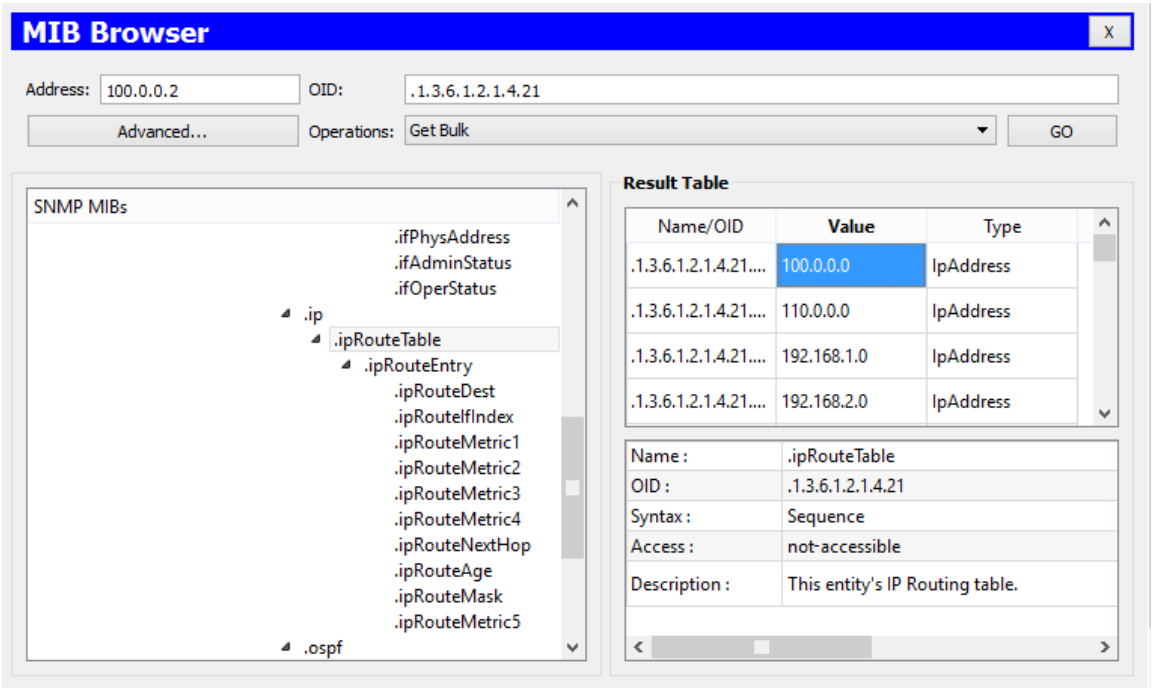


Fig. VI.13 Obtención de la tabla de enrutamiento vía NMS.

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

Gateway of last resort is not set

C    100.0.0.0/8 is directly connected, FastEthernet0/0
C    110.0.0.0/8 is directly connected, FastEthernet0/1
O    192.168.1.0/24 [110/2] via 100.0.0.1, 00:01:30, FastEthernet0/0
O    192.168.2.0/24 [110/2] via 110.0.0.2, 00:01:30, FastEthernet0/1
R_INTERMEDIO#
```

Fig. VI.14 Obtención de la tabla de enrutamiento *router* mediante la interfaz CLI del IOS.

Para corroborar los OID, relacionados con equipos CISCO, se puede consultar la herramienta gratuita de Cisco, "SNMP OBJECT NAVIGATOR". Uno de los ejemplos se visualiza en la figura VI.15 para "link down" (enlace caído), mientras que la herramienta se puede consultar vía web en la siguiente liga: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do

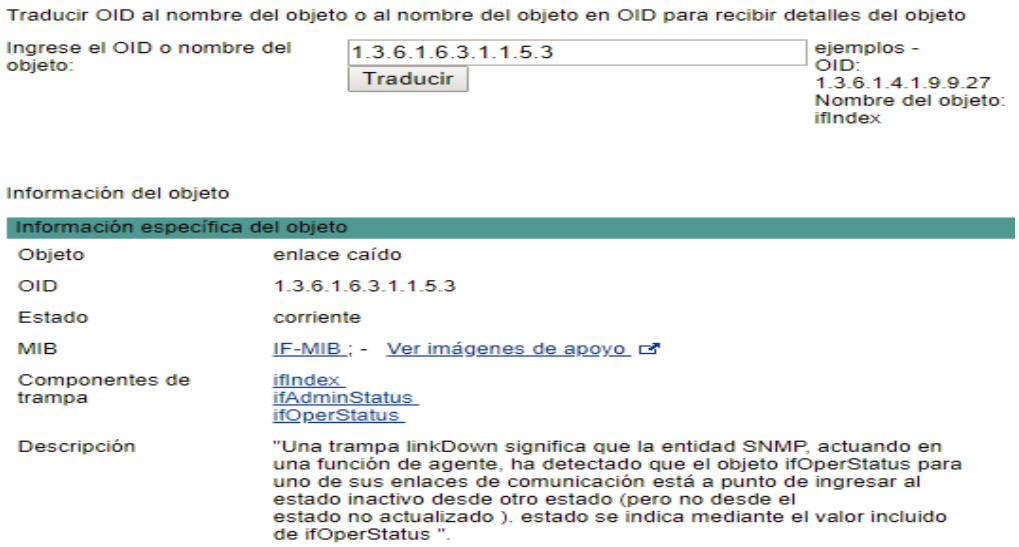


Fig. VI.15 Detalles del OID en el "SNMP *Object Navigator*" de Cisco.

También es posible obtener el estado de los enlaces, las tarjetas de red, así como detectar el estado de sensores de temperatura, ventiladores de las fuentes de alimentación, tarjetas de memoria y de

algunas otras variables que son monitoreadas. Otros buenos ejemplos para que el lector pruebe en la herramienta de Cisco, podrían ser:

OID: 1.3.6.1.4.1.9.9.13.1.3.1.2;
OID: 1.3.6.1.4.1.9.9.13.1.3.1.3;
OID: 1.3.6.1.4.1.9.9.13.1.3.1.6

El ejercicio anterior bien puede ser un excelente ejercicio académico, pero también se aplica ampliamente en diseño y desarrollo de TRAPS, alarmas y gestión vía SNMP, para cualquier equipo, no necesariamente Cisco (podría ser Lucent, Alcatel, Juniper, Nortel, Motorola, etc.) y tales aplicaciones son muy útiles en la industria de las telecomunicaciones, o para las empresas que sólo se dedican a la administración de esta tecnología.

VI.4 Sistemas de gestión comerciales: MIB Browser

Con la finalidad de que el lector pueda tener contacto con un MIB browser comercial, se recomienda descargar y probar diferentes MIB browsers comerciales, la mayoría de ellos tiene una versión gratuita.

Ireasoning

La versión personal del "MIB Browser" Ireasoning, de la compañía Ireasoning networks, se puede descargar desde https://www.ireasoning.com. El instalador pesa aproximadamente 37 MB y la instalación, por default se ubica en *C:\Program Files (x86)\ireasoning\mibbrowser,* con un peso aproximado de 130 MB. La figura VI.16 muestra algunos detalles de la instalación.

(a) archivo setup (b) Inicio de instalación

(c) Logo (d) Detalles de versión

Fig. VI.16 Generalidades para la instalación del MIB browser Ireasoning.

Una vez que usted ha instalado el "Ireasoning MIB Browser" puede, por ejemplo, solicitar el nombre de su *router* en la red en la que se encuentra. Si supongo que me encuentro en una red casera e indico la dirección de mi *router* para el OID correspondiente al *sysname*, observe la figura VI.17.

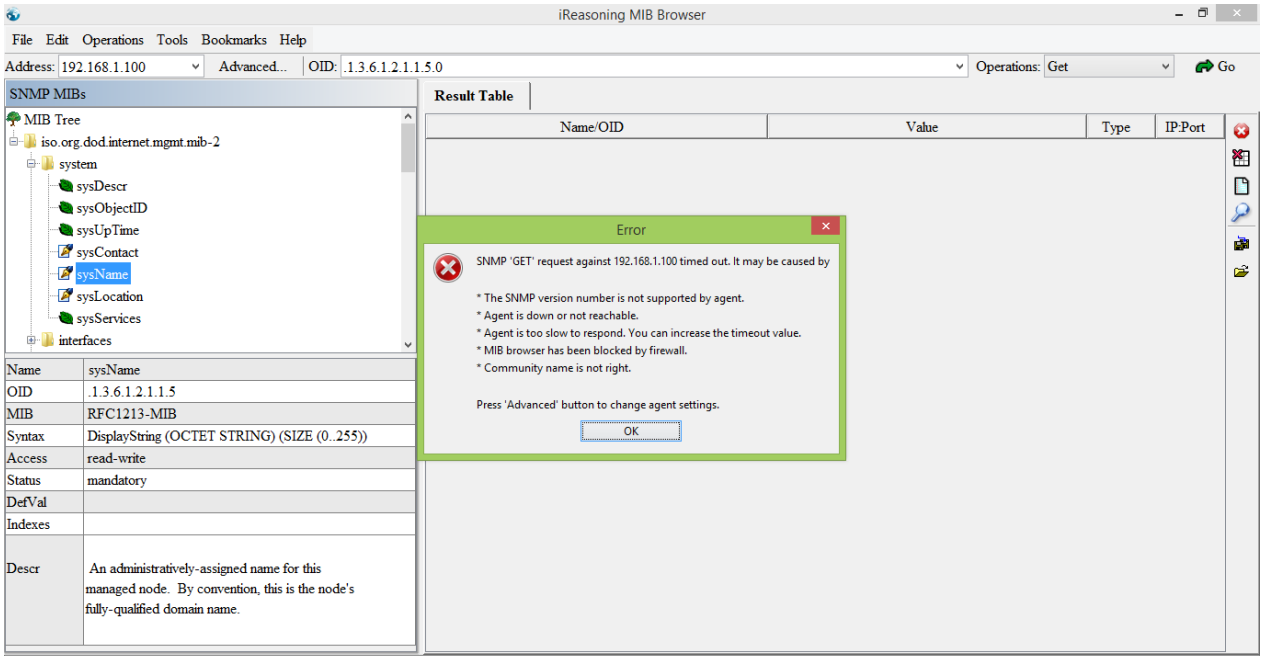


Fig. VI.17 Solicitud de nombre de sistema, en este caso del *router*.

¿Cuál es el motivo por el que no se obtuvo el resultado deseado?

Si no obtengo el nombre del *router*, tal vez se deba a que no he activado el agente SNMP en el *router*, o no he configurado el nombre de comunidad en el *router*.

Este software será de utilidad para cuando nos encontremos en una red que cuente con varios *routers* y, como administradores, podamos hacer las configuraciones correspondientes, tanto de los agentes, como de la comunidad, tal y como se ha indicado en el simulador. La figura VI.18 muestra los detalles y parámetros para solicitar información al agente de un *router*, para lo cual se requiere la dirección IP en la que se ubica al *router*, la versión de SNMP y las comunidades de lectura y escritura.

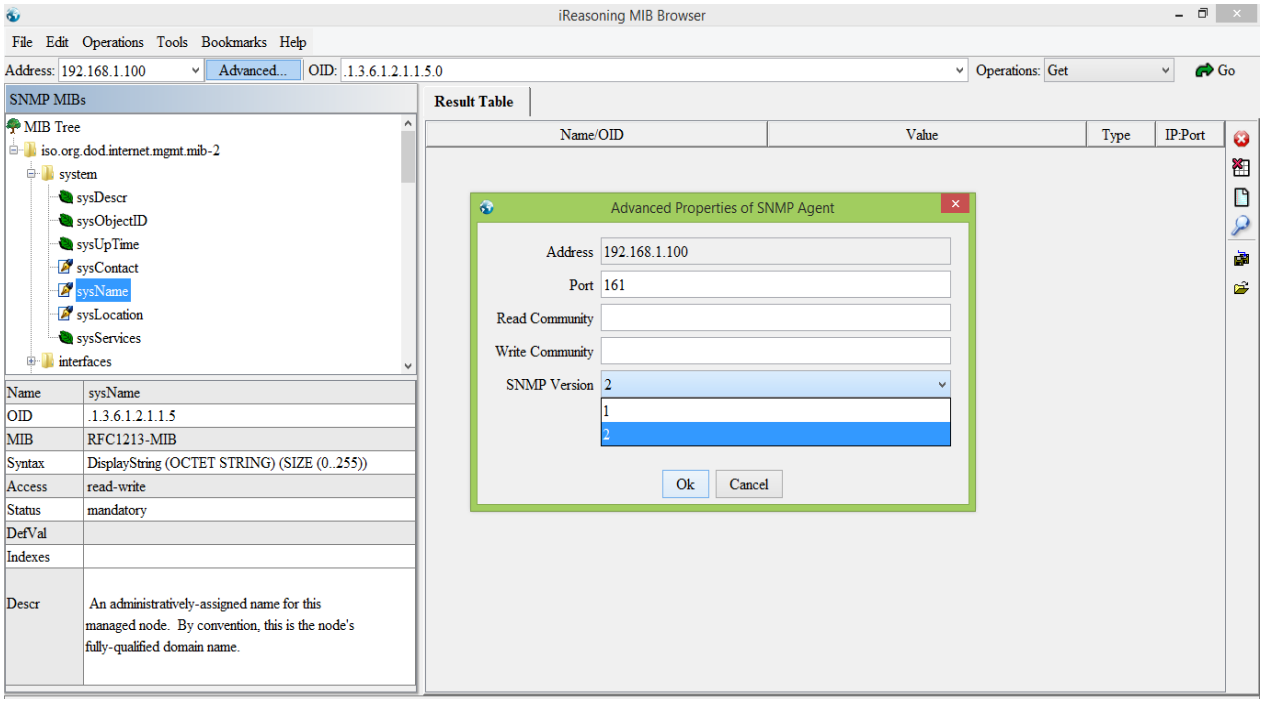


Fig. VI.18 Detalles para la solicitud de información a un agente en Ireasoning.

La figura VI.19 presenta un gran parecido al simulador de Packet Tracer, como en la figura VI.8, pero esta versión sí maneja los protocolos SNMPv1 y v2; no como el MIB browser del simulador Cisco Packet Tracer, el cual sólo maneja SNMPv1 y SNMPv2, aun cuando su persiana indica que maneja también la V3. El error se puede observar, ya que aun solicitándole que maneje la V3, sigue pidiendo *community name*, cuando debería solicitar las contraseñas para *privacy* y *security*.

Supongamos ahora que podemos acceder a una red en la que se encuentra un *router* con una gran cantidad de interfaces y es posible utilizar Ireasoning. Entonces, también será posible obtener el estado de la operación de las interfaces, como se indica en el resultado de la figura VI.19, en la que podemos observar el OID correspondiente a la variable *ifOperStatus;* esto para cada una de las 10 interfaces con las que cuenta un determinado *router*. Para esto se solicitó una operación GETBULK, la cual, como hemos visto, trae un conjunto de datos en formato de tabla.

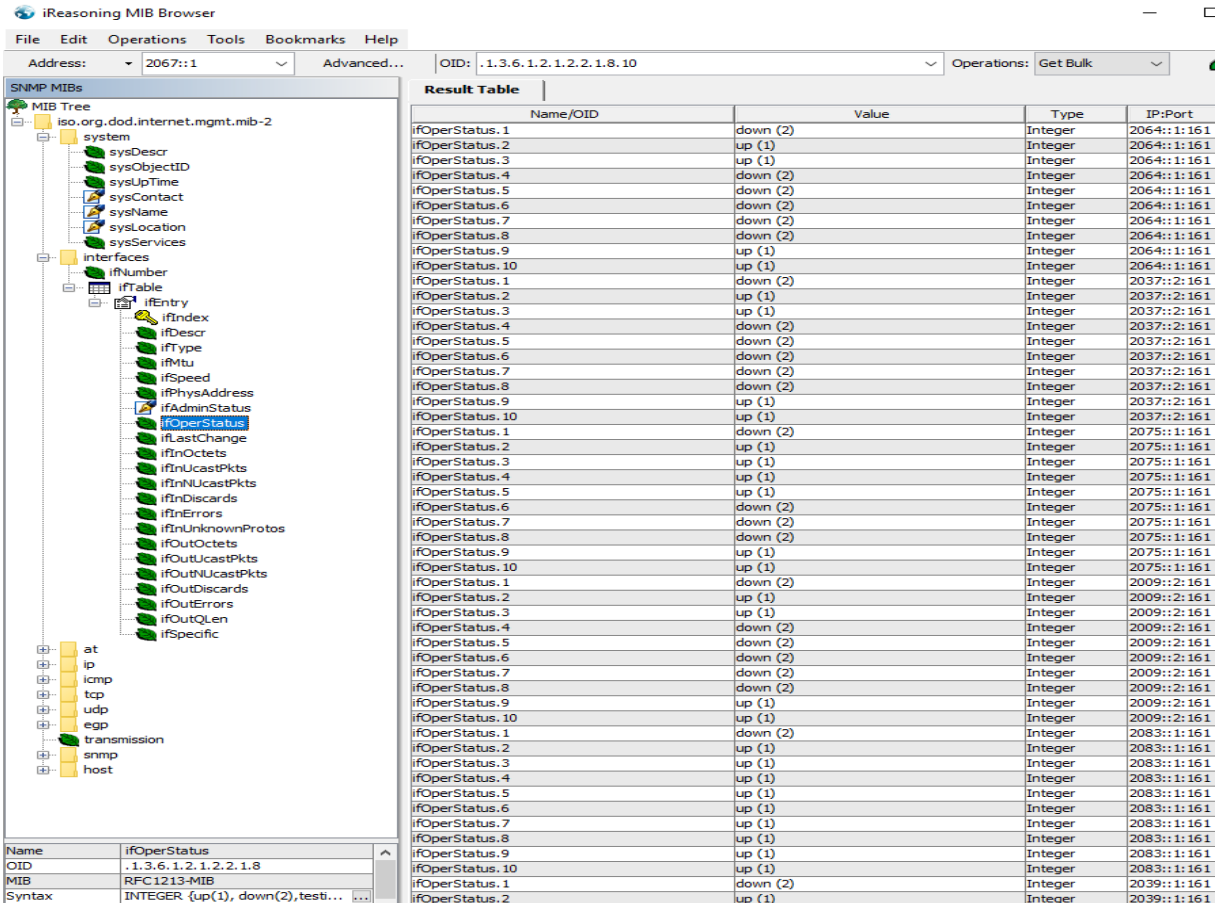


Fig. VI.19 Resultado de solicitar el estado de operación de las interfaces en un *router*.

Cuando se usa SNMPv3, se observa, en el software comercial “Power SNMP Free”, que sí es posible indicarlo con “privacy y security”, como se muestra en la figura VI.20.

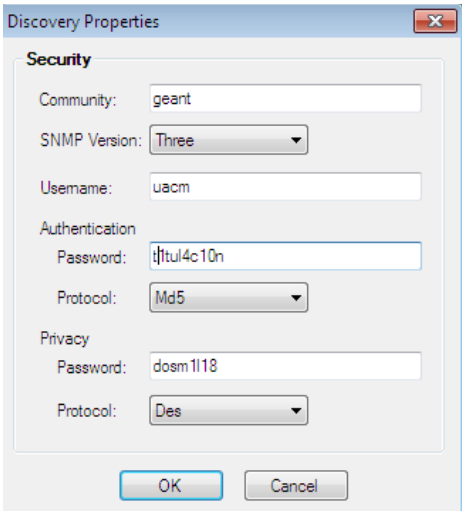


Fig. VI.20 Interfaz que muestra la configuración de un agente en SNMPv3.

Entonces, una vez configurado un agente bajo SNMPv3, sus paquetes pueden visualizarse en la figura VI.21, en la cual se pueden observar la versión y las características para autentificación y privacidad.

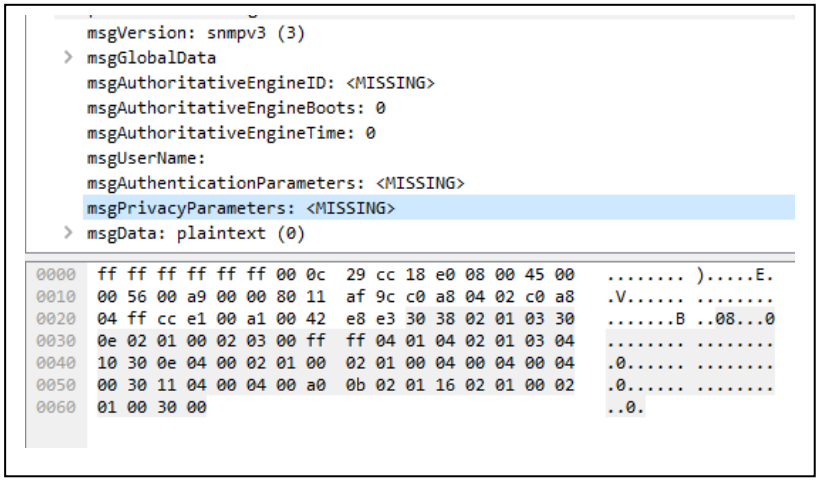


Fig. VI.21 Resultado de solicitar el estado de operación de las interfaces en un *router*.

PRTG Network Monitor (1997-Alemania)

Este sistema utiliza el protocolo “Syslog”. Las distintas versiones, gratuitas o de paga, depende del número de licencias; para ello se necesita una media de 5-10 sensores por dispositivo o un sensor para cada puerto de switch. La versión gratuita permite el uso de 100 sensores y se puede obtener desde la siguiente dirección: https://www.paessler.com/

NAGIOS Network Analyzer (2007-USA)

Este analizador y MNS se puede descargar desde la siguiente dirección: https://www.nagios.com/downloads/nagios-network-analyzer/

CACTI (2004)

Se puede obtener desde la siguiente dirección: https://www.cacti.net/

ZABBIX (2004)

Se puede obtener desde la siguiente dirección: https://www.zabbix.com/about

VI.5 PRÁCTICA 7: Gestión

El objetivo de esta práctica es que usted desarrolle habilidades de gestión de redes, una vez que ya ha desarrollado las habilidades necesarias y adquirido los conocimientos para proveer la conectividad de una red, para lo cual usted ya ha trabajado lo suficiente en las 6 prácticas anteriores.

Actividad 1: Dada la figura IV.34, "Topología física para 9 redes con 8 *routers*: Caso México", simule la infraestructura de la red MAN de modo que realice la gestión de cualesquiera de los *routers* de la red, empleando 5 pruebas, desde una de las computadoras que usted elija para que haga las veces de NMS.

Actividad 2: Dada la figura IV.35, "Topología física para 17 redes con 16 *routers*: Caso México", simule la infraestructura de la red MAN de modo que realice la gestión del *router* CDMX de la red, empleando 5 pruebas, desde la computadora que usted elija para que funcione como NMS.

Nota anecdótica profesional

El 100% del material contenido en este capítulo tiene aplicación práctica en la industria de las telecomunicaciones y en particular en las empresas ISP, particularmente en aquellas áreas donde se aplica alta tecnología para las redes de backbone. Ello se deriva de mi experiencia profesional en REDUNO Telmex y al interrelacionarme con CISCO, Alcatel, Lucent, y Juniper, en el laboratorio de "cambio tecnológico", donde hacíamos la transferencia tecnológica, probábamos exhaustivamente SNMP y de manera particular *traps* como alarmas. Con el tiempo aparecieron sistemas de gestión muy especializados, para ISP de alta complejidad. Entre ellos, usamos un software de origen israelí llamado "Sheer", el cual posteriormente fue comprado por CISCO y renombrado como ANA. Entre los años 2006 a 2008, el software era de tal complejidad y costo, que sólo dos ISP en el mundo contaban con él, *Deutsche Telekom* de Alemania y RedUno-Telmex de México. El sistema *Sheer* fue desarrollado con base en avances de un sistema militar de defensa del ejército de Israel, y una parte fue acondicionada para telecomunicaciones, por la empresa que desarrollo el mencionado sistema.

VI.6 EVALUACIÓN PARTE III

Tiempo máximo: 60 minutos. Lea cuidadosamente. El instrumento contiene reactivos del nivel cognitivo "recordar" (conocer), cuyo valor es 1 punto y, reactivos del nivel cognitivo "comprender", cuyo valor es 2 puntos.

Parte I Gestión (10 pts.)

1. Defina agente (1pt.)

_____

_____

2. Bosqueje el formato de SNMP v1 e indique sus componentes relevantes (2pts)
3. Bosqueje el formato de SNMP v2 e indique sus componentes relevantes (2pts)

Suponga que se encuentra en contacto con la CLI de un *Router*

4. Configurar en el *router* SNMPv2, use las claves que usted desee (2pts).

```
Router#
```

5. De todos los OID que usted manejó, indique el nombre de 4 objetos (1 pt.)

A)_____B)_____

C)_____D)_____

6. Liste 3 sistemas de gestión comerciales (1 pt.)

a) _____ b) _____ c) _____.

7. Explique brevemente la diferencia entre SNMPV1 y SNMPv2 (1 pt.).

_____

_____

PARTE IV: REDES AVANZADAS

CAPÍTULO VII: INTRODUCCIÓN A LAS REDES AVANZADAS

Internet es como un gran fractal, hacia arriba y hacia abajo, así es como lo veríamos quienes observamos las áreas exactas y naturales. En el caso de las ideas, una idea origen lleva a otra, de la cual surge otra idea y, esta, genera a otra y así "ad infinitum". A la fecha, la deseada red intergaláctica, que se convirtió en la Internet, tiene viviendo a la Internet 1, la Internet 2 y la Internet Interplanetaria. Experimentar con la infraestructura de backbone de una red avanzada es sumamente caro y queda restringido para los laboratorios de transferencia tecnológica y los entornos de pruebas, que sólo poseen las compañías proveedoras de internet; por lo que en la academia se requiere del uso de simuladores y emuladores.

Entonces, ¿cuál es el estado actual de la producción académica mundial en redes avanzadas?

¿Cuánto aporta ADVNETLAB de la UACM a la ingeniería en México y a las redes avanzadas?

VII.1 Simulación *vs* emulación

Un **simulador** es un programa que busca asemejarse al funcionamiento de un sistema real, pero no presenta un control real ni una adquisición de datos reales, de modo que nunca podría igualar el desempeño de un equipo o un sistema real.

Por ejemplo, la "simulación Montecarlo" es un método estadístico que se usa para resolver problemas matemáticos de cierta complejidad, generando variables aleatorias. Esta simulación inició aplicándose a juegos de casino, como tirador de dados y la ruleta. El método Montecarlo usa un muestreo aleatorio reiterativo para obtener la probabilidad de una determinada serie de resultados y predecir las posibilidades de un evento incierto. Este método se inventó, durante la segunda guerra mundial (1939-1945), por parte de John von Neumann y Stanislaw Ulam. En el caso de la economía, los simuladores no pueden predecir cómo se va a comportar un determinado sistema, pero se aspira a obtener resultados aproximados, como en el caso de la bolsa de valores. Este método se usa en electrónica para los simuladores de diodos, transistores y circuitos; los modelos se aproximan a comportamientos generales en intervalos lineales y aproximaciones sucesivas o exponenciales. La simulación podría dar alta precisión, pero baja exactitud. En el método Montecarlo, si un programa intenta generar números aleatorios, en realidad obtendrá números pseudoaleatorios, porque se usan ecuaciones que parecen emplear variables aleatorias, pero en realidad no lo son. "Excel" y "Matlab" usan simulación Montecarlo, así como el "IBM SPSS *statistics*", entre otros **[48]**. En el caso de los simuladores de vuelo y simuladores de ciudades se consideran algunas variables, pero hay muchas variables que no están consideradas. Específicamente para el caso de redes quizás el simulador más popular es el Cisco *packet tracer*, el cual, por ejemplo, no cuenta con equipos de backbone de la familia c7200.

Un **emulador** imita, iguala o mejora el funcionamiento de un equipo o sistema. Un emulador podría dar "alta precisión y alta exactitud", es decir, se comporta como un sistema real pero no lo es. Por ejemplo, en el caso del "emulador GNS3", cada vez que se emula una computadora, se debe cargar el sistema operativo real que se instala en una computadora, tal como Linux, Windows, OS2, o Unix, y esto es algo que no puede ocurrir en un simulador, por ello utiliza una cierta cantidad de memoria RAM y CPU **[49]**. Y, cada vez que se emula un *router* CISCO, se debe cargar el IOS real que se usa en los *routers*, para lo que se utiliza una determinada cantidad de memoria RAM y de CPU. La figura VII.1 muestra la interfaz del emulador GNS3, en el que se

presentan *routers* de acceso y el de backbone de la familia C7200. La figura VII.2 muestra un equipo C7200 del laboratorio ADVNETLAB.

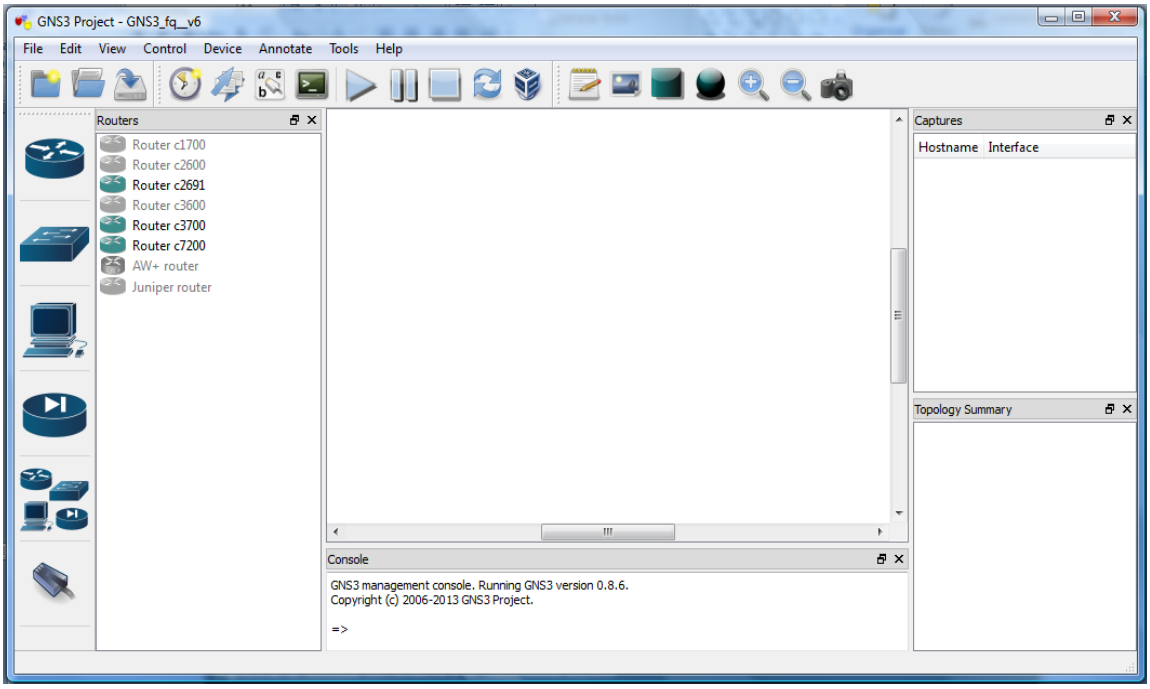


Fig. VII.1. Emulación de la topología del *backbone* de Internet 2 con GNS3.

Fig. VII.2. Emulación de la topología del *backbone* de Internet 2 con GNS3.

VII.2 Las redes avanzadas: Internet 2 en el mundo

Desde 1969, hasta 1990 que se apagó la ARPANET y hasta 1995 que se mantuvo la NSFNET como red dominante. Esa Internet fue una red experimental con una conexión comercial, de modo que una vez que se dejó como una Internet completamente comercial en 1995 y que, debido a su crecimiento exponencial y al incremento de su complejidad, el gobierno de EUA liberó su control, entonces fue necesario crear una red alternativa en la que se pudiese seguir experimentando. Una vez que la Internet se vuelve comercial, ya no es posible hacer pruebas, pues los ISP son dueños de sus propias infraestructuras, de modo que los clientes corporativos y residenciales no verían bien apagones en la Internet comercial que contratan.

Así es como, en 1996, se crearon en los EUA un conjunto de redes similares a Internet, bajo la topología distribuida de la NSFNET, para la experimentación, la investigación, y para cubrir aspectos de educación, como se había concebido a la red en un inicio, y así cada uno de los países implementó una red alternativa a la que llamamos Internet 2.

La Internet 2 se implementa en cada país con equipos de backbone idénticos a los usados en la Internet 1 o Internet comercial, pero al no tener usuarios residenciales, ni corporativos se cuenta con una red de alta velocidad. La Internet 2 era necesaria para seguir realizando pruebas y futuros desarrollos para protocolos y funcionalidades que permitan mejorar la Internet comercial u otras posibles versiones. Esa nueva Internet que quedó dentro de universidades y centros de educación o investigación. Y así como la internet comercial es la integración de las redes que cada empresa o país va agregando como una contribución colectiva, con el tiempo las redes de Internet II recibieron el nombre de redes avanzadas, al dedicarse a universidades y centros de investigación, se les llama también Redes Nacionales para la Investigación y la Educación (*National Research and Education Network* - NREN); incluso, en algunos casos, se le llama la "Internet de la siguiente generación", dado que se sigue experimentando con ellas. A toda internet la podemos modelar de acuerdo con la ecuación 1, como una colección de sistemas autónomos, de modo que cada nueva compañía proveedora de Internet, con su propio sistema autónomo, agrega más y más infraestructura a la Internet **[50]**.

$$Internet = \sum_{i=1}^{n} AS_i \tag{1}$$

Donde "n" es el número total de sistemas autónomos, y "AS" los sistemas autónomos

(*Autonomous Systems*).

En cada país existe un determinado número de compañías ISP o CSP, las cuales proveen Internet comercial; sin embargo, sólo algunas de ellas son las que proveen servicios de conexión a las redes avanzadas.

En el caso de México, mi primera experiencia directa con Internet 2 fue para hacer un dictamen técnico solicitado por la rectoría de la UPAEP (universidad en la cual yo era profesor investigador de tiempo completo), ya que se quería conocer los detalles y beneficios para que se hicieran las inversiones pertinentes y la UPAEP ingresara al consorcio que maneja Internet 2 en México **[51]**.

¿Para qué se usa la Internet 2?

En los medios de investigación hay relación con instituciones académicas y con centros de investigación, públicos y privados, que principalmente estudian problemas de salud, para analizar de manera colectiva problemas, como Alzheimer, demencia senil, y neuropatías. Pero también hay especialistas centrados en astronomía, en el que Chile juega un papel importante con sus catorce centros astronómicos; incluso, en el caso de la física de partículas el gran colisionador de hadrones en el *European Organization for Nuclear Research* (CERN) se apoyan de esta red alternativa de Internet **[52-54]**.

VII.3. INTERNET 2- EUA

La Internet 2, es decir, la red avanzada de EUA tiene una evolución interesante, pero lo que da relevancia a esa red, en términos de infraestructura es la evolución de su backbone, tanto en los equipos *routers* de backbone como su topología y sus anchos de banda, que la hacen una red de alta velocidad. Nuevamente, cabe aclarar que estas redes no están disponibles para el público en general, sólo se puede acceder a ellas desde centros de investigación, públicos o privados, o desde instituciones de educación superior que sean miembros de los consorcios en cada país y que paguen su membresía a ese organismo, cubriendo el costo de los servicios de interconexión a las compañías que brindan el servicio de ISP. En la figura VIII.3 se muestra la topología del backbone de la Internet 2, la cual ha sido emulada en GNS3 con equipos de backbone Cisco 7200, utilizando el IOS de los equipos reales. Con la finalidad de que el lector revise todos los detalles, favor de consultar el artículo correspondiente a la referencia [55]. Con la finalidad entender su funcionamiento, se realizan pruebas de conectividad entre todos los equipos de *backbone* y posteriormente de gestión, poniendo atención a las respuestas de los protocolos en el uso del ancho de banda y la latencia. Internet 2 cuenta actualmente con anchos de banda, en su *backbone,* de 100 Gbps y en algunos tramos, hasta los 1000 Gbps.

Fig. VII.3. Emulación de la topología del *backbone* de Internet 2 con GNS3.

VII.4. CANARIE – Canadá

La NREN canadiense evolucionó hasta llegar a CANARIE, la cual a su vez inicia, en 1998, con un ancho de banda de 1Gbps **[56, 57].**

En la figura VII.4 se muestra la topología del backbone de CANARIE, la cual ha sido emulada en GNS3 con equipos de backbone Cisco 7200 utilizando el IOS de los equipos reales. Con la finalidad de que el lector revise todos los detalles, favor de consultar el artículo correspondiente a la referencia **[58]**. Desde 2016, CANARIE tiene un ancho de banda de 100 Gbps.

Fig. VII.4. Emulación de la topología del *backbone* de CANARIE con GNS3.

VII.5. CLARA – Latinoamérica

En 1998 varios países latinoamericanos interconectaron sus redes avanzadas pequeñas, comparadas con las de EUA y Canadá, y las agruparon en un consorcio llamado CLARA, como acrónimo de **C**onsorcio **La**tinoamericano de **R**edes **A**vanzadas [59]. En la figura VII.5 se muestra la topología del *backbone* de CLARA, la cual ha sido simulada en *packet tracer* con equipos de acceso Cisco. Con la finalidad de que el lector revise todos los detalles, favor de consultar el artículo correspondiente a las referencias [60, 61].

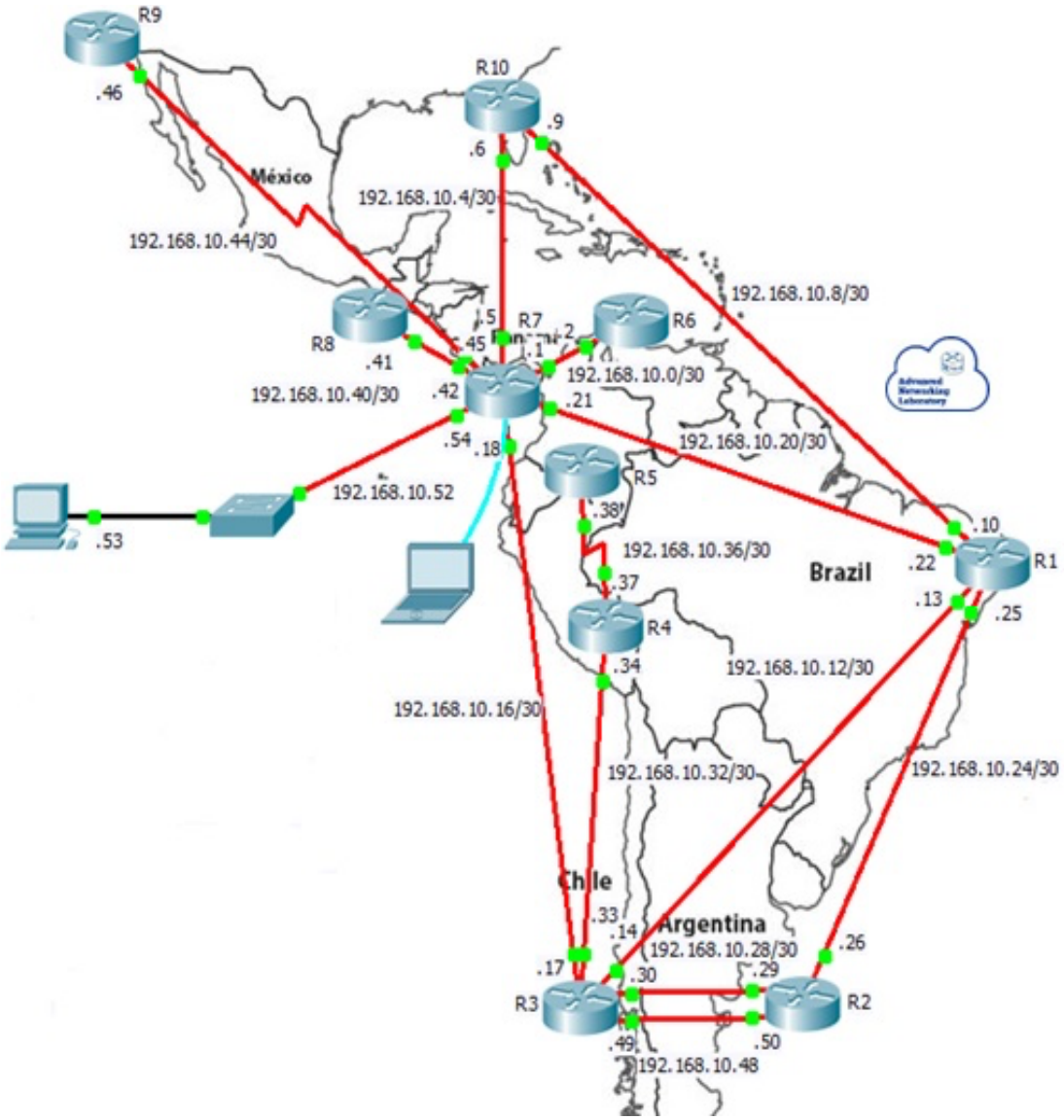


Fig. VII.5. Simulación de la topología del *backbone* de CLARA con Packet Tracer.

En la figura VII.6 se muestra la topología del backbone de CLARA, la cual ha sido emulada en GNS3 con equipos de backbone Cisco 7200, utilizando el IOS de los equipos reales. Con la finalidad de que usted revise todos los detalles, favor de consultar el artículo correspondiente a las referencias **[60, 61]**. Esta topología, como las anteriores, es importante como un refernte, ya que el lector podrá hacer simulaciones y emulaciones de las topologías de backbone, buscando reproducir la conectividad y gestión como se indica en los artículos citados.

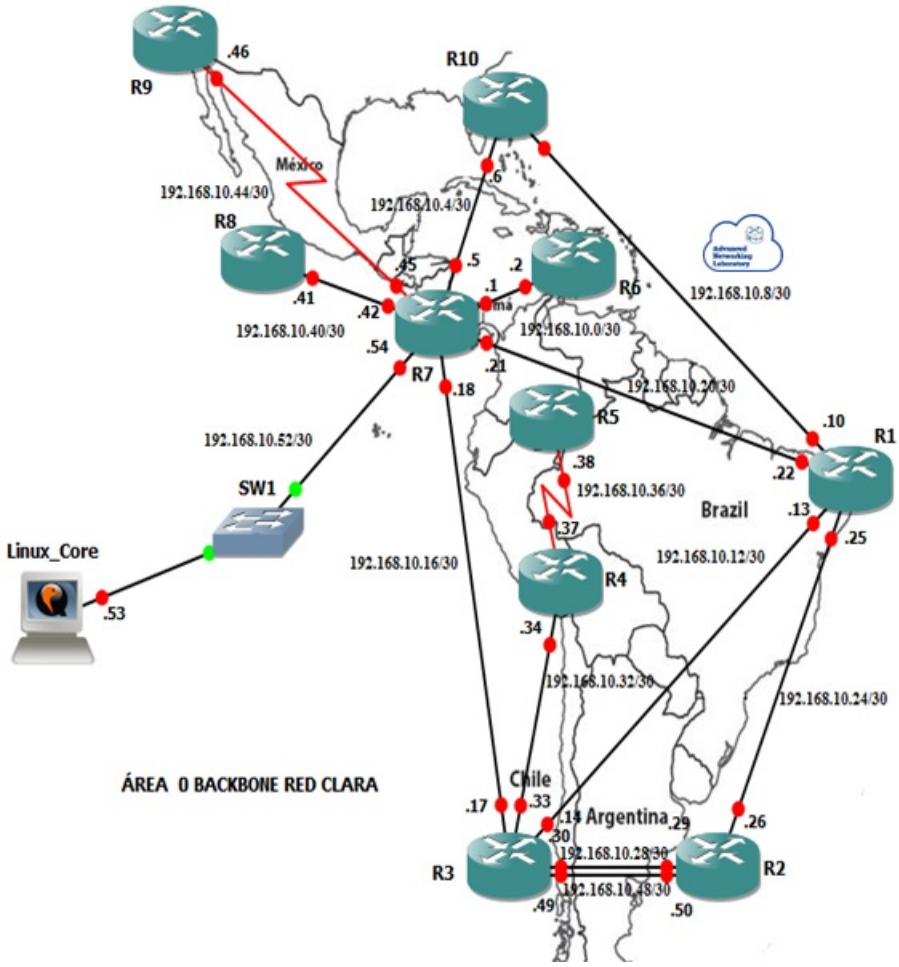


Fig. VII.6. Emulación de la topología del *backbone* de CLARA con GNS3.

VII.6. CUDI – México

En México, Internet 2 está coordinado por el Consorcio Universitario para el Desarrollo de Internet 2 (CUDI), el cual nació el 8 de abril de 1999. El objetivo de Internet 2 en México es:

Promover y coordinar el desarrollo y difusión de aplicaciones de tecnología avanzada de redes de telecomunicaciones y cómputo en México, enfocadas al desarrollo científico y educativo de la sociedad mexicana, así como el desarrollo de la infraestructura para que tales aplicaciones se lleven a cabo". Desde el año 2000, se desarrollan al menos 2 reuniones del CUDI por año, en las que se discuten los avances en materia de Internet 2 (abreviado como I2). La arquitectura de I2 en México se compone de 4 niveles: **[1, 62].**

1. **Enlaces internacionales:** México se conecta con dos enlaces físicos: uno, vía Tijuana a San Diego, California, (Nodo California) para las redes CENIC, ABILENE y CLARA (Cooperación Latino Americana de Redes Avanzadas), y el otro, vía Ciudad Juárez (Nodo Houston) para las redes VBN y ABILENE.
2. **Nivel dorsal (BB-Backbone)** (infraestructura mexicana: SW y router): Los routers de backbone están indicados en la tabla VII.1, a los que se agregan 4 switches SW-BPX8600. Para ello, las empresas Telmex y Avantel (comprada por Axtel) colocaron 4 km de FO. El ancho de banda del backbone es de STM 1=155 Mbps.

Proporcionados por TELMEX	Proporcionados por AXTEL (antes AVANTEL)
Nodo DF - Cisco 7206	Nodo DF - GSR 10000 (**cambio**)
Nodo MTY- Cisco 7206	Nodo MTY- GSR 10000 (**cambio**)
Nodo Tijuana - Cisco 7206 (Por donde también se sale a CLARA y CENIC)	Nodo Cancún- Cisco 7200
Nodo Juárez- Cisco 7200	Nodo DF I2 Cisco 7513
Nodo Guadalajara - Cisco 7206	DF- Cisco 7606

Tabla VII.1 *Routers* para el BB de CUDI o I2 en México desde 1999 hasta 2007.

3. **Nivel Asociados:** 22 enlaces asociados, con enlaces E3 de nodos de agregación (11 equipos proveídos por Telmex y 9 equipos proveídos por Avantel, hoy Axtel)
4. **Nivel Afiliados:** Administración de 22 conexiones de tránsito a redes académicas hasta 2004.

La figura VII.7 muestra cómo se encontraba la arquitectura de I2 en México hasta 2004.

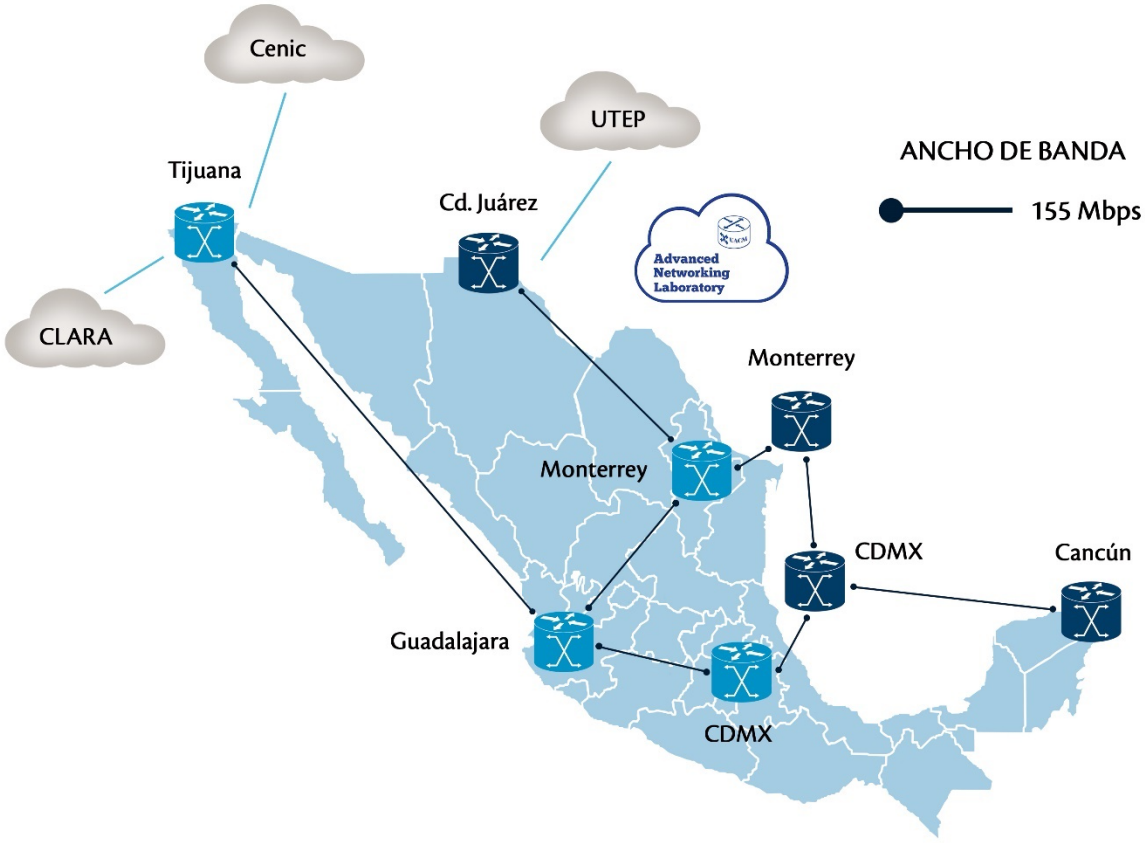


Fig. VII.7. Topología fundacional de CUDI, Internet 2 en México, año 2004.

El NOC-CUDI (*Network Operations Center*) tiene por objetivo la administración, control, monitoreo y operación de toda la infraestructura física y lógica, que conforma la dorsal de la red CUDI, para asegurar el óptimo desempeño de la red. Las 6 funciones del CUDI, realizadas por 3 personas (2CUDI + 1 UNAM, institución a cargo del NOC-CUDI), son: Monitoreo, ingeniería, operación/soporte, análisis/configuración, administración de software, atención y seguimiento de fallas. Para realizar tales tareas el NOC cuenta con: WS SUN, Servidor Linux Dell *WS Precision*, para páginas WEB y Help Desk; servidor Unix SUN SunFire V250 Monitoreo de red (como Network Management Station); un switch de 12 puertos 100/1000 UTP y 3 PC para tres personas, dos de CUDI y 1 UNAM. El CUDI es el Internet 2 en México y existen consorcios similares en cada país, bajo la denominación de redes avanzadas. La figura VII.8 muestra cómo se encontraba la arquitectura de I2 en México, incluyendo los anchos de banda y las principales instituciones fundadoras **[1, 62]**.

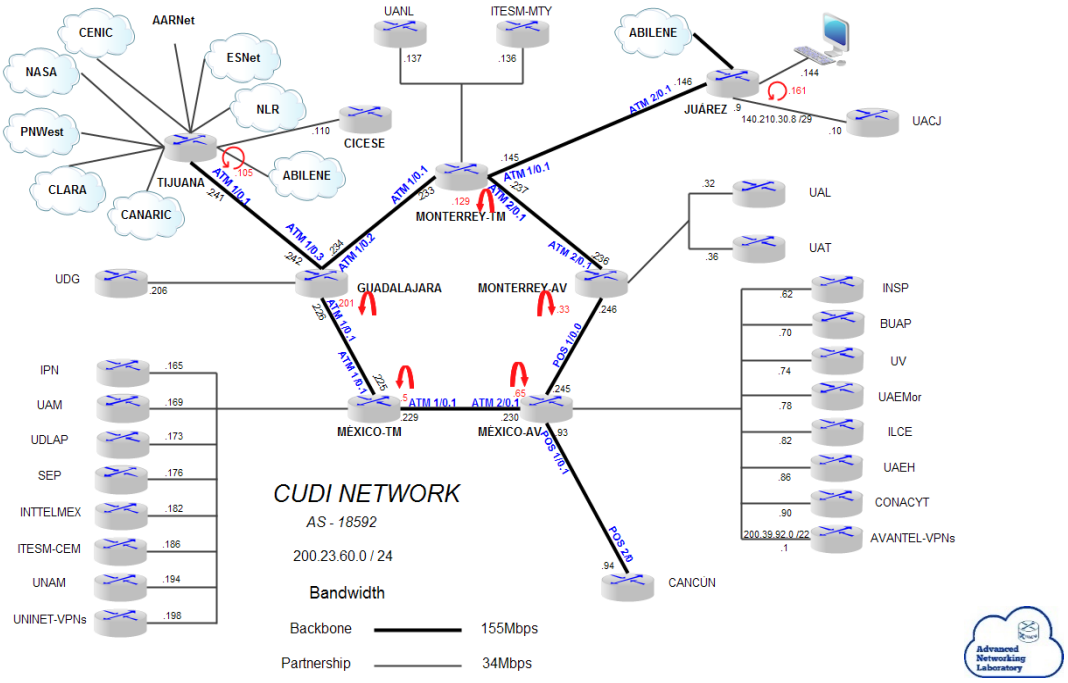


Fig. VII.8. Topología del *backbone* de Internet 2 en México con velocidades e instituciones.

La figura VII.9 muestra la simulación de la topología de CUDI en *packet tracer*, con la limitación de que este simulador no maneja los *routers* de *backbone* de la familia c7200 [50].

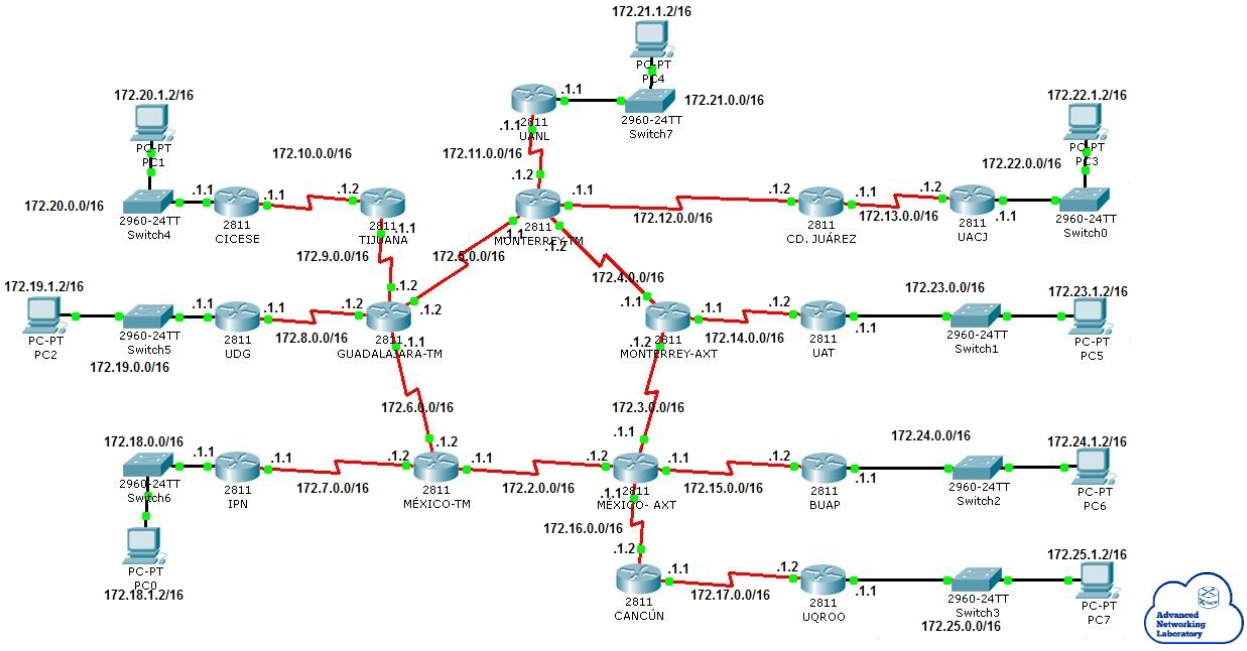


Fig. VII.9. Simulación de la topología del *backbone* de CUDI con *packet tracer*.

Es entonces cuando se hace necesario realizar una emulación, para lo cual se puede usar el emulador GNS3. Así, la figura VII.10 muestra la emulación de CUDI, en la que se observan los *routers* de *backbone* de la familia c7200. También se observan las máquinas virtuales con base en Linux **[50]**.

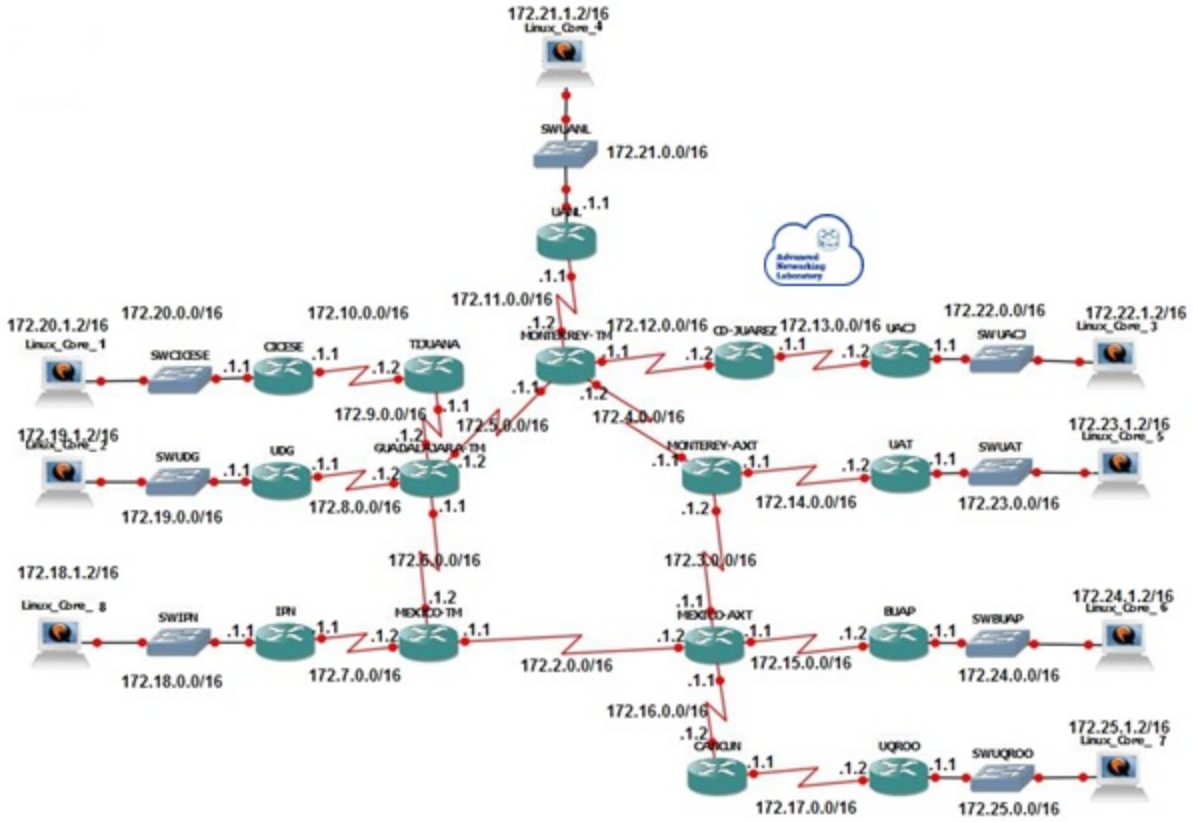


Fig. VII.10. Emulación de la topología del *backbone* de CUDI con GNS3.

En el caso específico de México, existen 10 grandes empresas proveedoras de Internet comercial, las cuales tienen una cobertura en todo el país. Sin embargo, sólo 2 empresas dan servicios de Internet 2, exclusivamente para la red conocida como CUDI, una de ellas es REDUNO-Telmex; la otra inició como AVANTEL - una filial de AT&T en México – pero, al quebrar AVANTEL, se vendió todo a la compañía AXTEL.

VII.7. GEANT – Europa

Europa desarrolló una red avanzada, la cual ha evolucionado, como todas, actualizando sus equipos de backbone y sus anchos de banda, cambiando de nombres, mientras va agregando a más países de la Unión Europea **[63-65].**

En la figura VII.11, se muestra la topología del backbone de la "red avanzada europea tipo gigabit" (***G**igabit **E**uropean **A**dvanced **N**e**T**work* - GEANT), la cual ha sido emulada en GNS3 con equipos de backbone Cisco 7200, utilizando el IOS de los equipos reales. Con la finalidad de que el lector revise todos los detalles, favor de consultar el artículo correspondiente a la referencia **[66]**. Esta topología es una referencia importante, ya que el lector podrá hacer simulaciones y emulaciones de las topologías de backbone, buscando reproducir la conectividad y gestión, como se indica en los artículos citados.

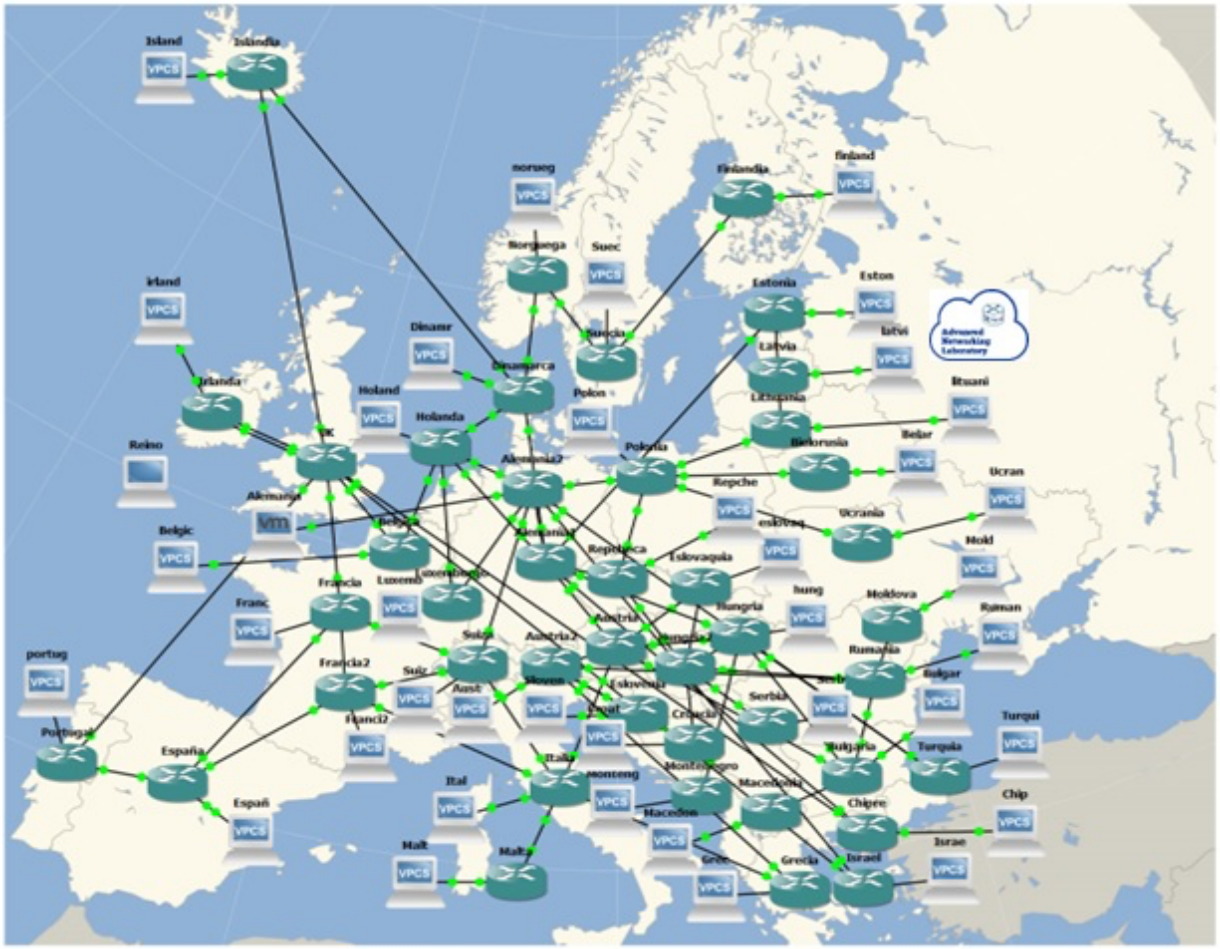


Fig. VII.11. Emulación de la topología del *backbone* de GEANT con 43 *routers* de *backbone*.

VII.8. AFRICACONNECT – África

Las redes avanzadas africanas han podido integrarse en una sola red, a partir de 3 redes regionales. AFRICACONNECT ha crecido desde su versión 1 a 4, impulsada por Europa, a la cual se conecta por 3 vías, por Reino Unido, Francia y Holanda, de modo que los países europeos mantienen un vínculo con sus antiguas colonias [67].

En la figura VII.12 se muestra la topología del backbone de la red AFRICACONNECT, la cual ha sido emulada en GNS3 con equipos de backbone Cisco 7200, utilizando el IOS de los equipos reales. Con la finalidad de que el lector revise todos los detalles, favor de consultar el artículo correspondiente a la referencia [68].

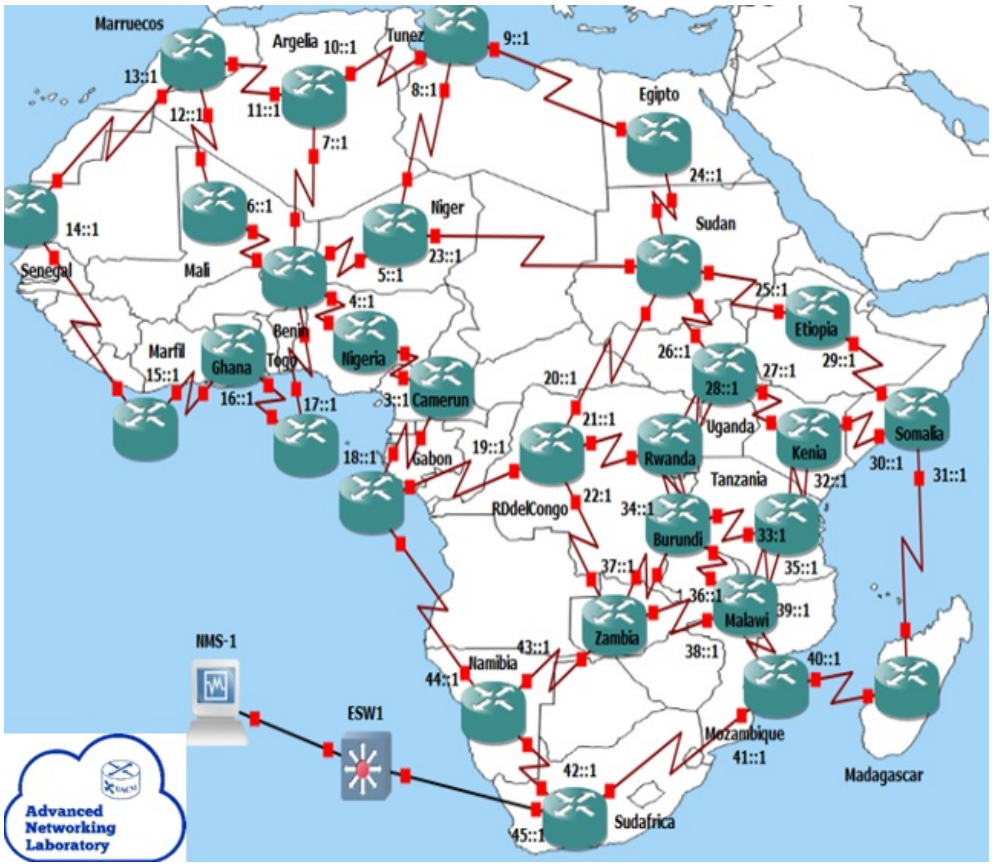


Fig. VII.12. Emulación de la topología del *backbone* de Africaconnect.

La tabla VII.2 muestra, a manera de resumen, las páginas web de las diferentes redes avanzadas tratadas aquí y algunas otras redes de importancia **[69-70]**.

RED AVANZADA	Sitio WEB
CANARIE	https://www.canarie.ca/network/
INTERNET2	https://www.internet2.edu/
CLARA (Consorcio Latino Americano de Redes Avanzadas)	https://www.redclara.net
CUDI (Consorcio Universitario para el Desarrollo de Internet)	www.cudi.mx
GEANT (Gigabit European Advanced Network)	https://www.geant.org/
AFRICACONNECT	https://www.africaconnect2.net
APAN (Asia Pacific Advanced Network)	http://apan.net/
CERNET (China Education and Research Network)	http://www.edu.cn/
Pacific wave	www.pacificwave.net

Tabla VII.2 Sitios web para cada una de las redes avanzadas mendionadas.

VII.9. Protocolo BGP

El protocolo de Gateway de frontera (*Border Gateway Protocol* - BGP) es el protocolo de enrutamiento diseñado para interconectar un AS con otros AS, por tanto, se considera un protocolo EGP, como se observó en la figura IV.1. Por lo anterior, a BGP se le considera un protocolo de enrutamiento de sistemas inter-autónomos, como se indica en la figura VII.13. Mientras que si hacemos un acercamiento a cada uno de los AS nos encontramos con los detalles indicados en la figura VII.14 [71].

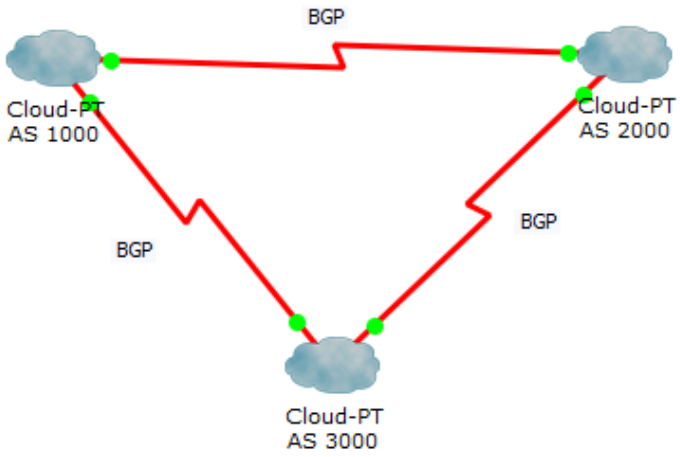


Fig. VII.13 Topología para redes de Sistemas Autónomos usando BGP.

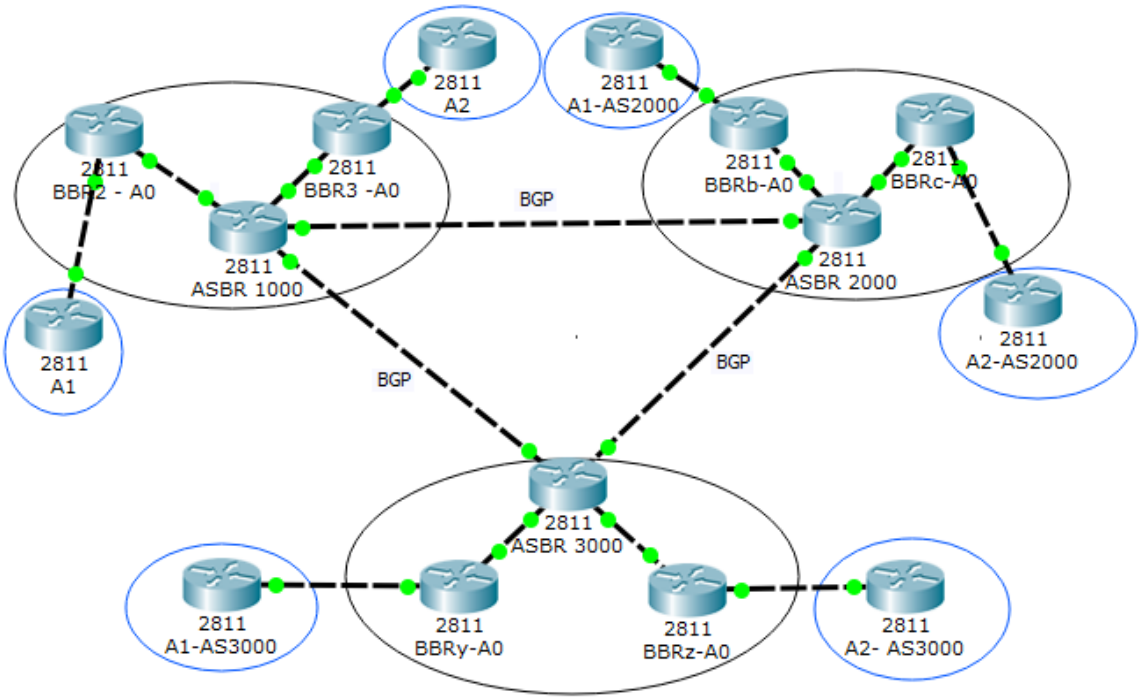


Fig. VII.14 Topología detallada de cada Sistema Autónomo.

En la figura VII.15 se muestra la manera de configurar al *router* ASBR 1000 (*Autonomous System Backbone Router*), el cual es el punto de contacto que da entrada al AS ((*Autonomous System*) número 1000. Previamente, se han configurado aquellas interfaces que se conectan a otros sistemas autónomos.

```
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to
up

Router(config-if)#exit
Router(config)#interface FastEthernet1/1
Router(config-if)#ip address 30.0.0.2 255.0.0.0
Router(config-if)#exit
Router(config)#router bgp 1000
Router(config-router)#bgp router-id 10.10.10.10
Router(config-router)#neighbor 10.0.0.2 remote-as 2000
Router(config-router)#neighbor 30.0.0.1 remote-as 3000
Router(config-router)#
```

Fig. VII.15 Configuración del *router* ASBR 1000.

A partir de este momento, habrá comunicación sobre las interfaces configuradas bajo el protocolo ARP para llenar las tablas arp, y de este modo, se podrían conocer las interfaces. Sin embargo, si los otros routers no se configuran como BGP, no habrá más comunicación.

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 2000
Router(config-router)#bgp router-id 20.20.20.20
Router(config-router)#neighbor 10.0.0.1 remote-as 1000
Router(config-router)#neighbor 20.0.0.2 remote-as 3000
Router(config-router)#
```

Fig. VII.16 Configuración del *router* ASBR 2000.

Entonces una vez que el *router* se haya configurado como BGP (como se muestra en la figura VII.17), podrá aparecer un paquete BGP, como el indicado en color morado, el cual viaja desde el AS 2000 hasta el AS 1000.

VII.9.1 Paquetes BGP

Los paquetes BGP contienen 9 campos: *Version number*, *Type*, *Packet length* (bytes), *Router ID*, *Area ID*, *Checksum, authentication type, Authentication* y *Data* **[71]**.

En el caso de los datos, pueden existir 4 tipos de datos o mensajes:

A) *Open*: Mensaje que se usa para iniciar una sesión BGP, una vez establecida una conexión TCP vía el puerto 179.

B) *Keepalive*: Mensaje que se envía periódicamente para confirmar que el otro extremo sigue activo en la sesión.

C) *Update*: Mensaje de actualización el cual contiene anuncios.

D) *Notification*: Mensaje que se envía al cerrar una sesión BGP.

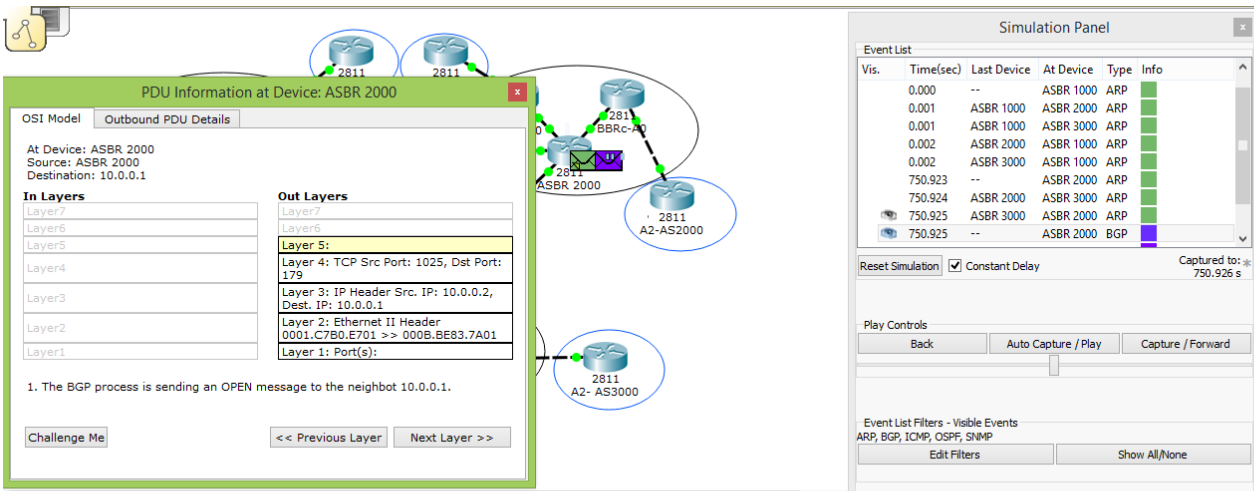


Fig. VII.17 Paquetes BGP desde el ASBR 2000 entre sistemas autónomos.

En la figura VII.18 observe cómo se envía un mensaje BGP OPEN, en su versión 4 y el número de sistema autónomo vía el paquete TCP, por el puerto 1025 hacia el puerto 179.

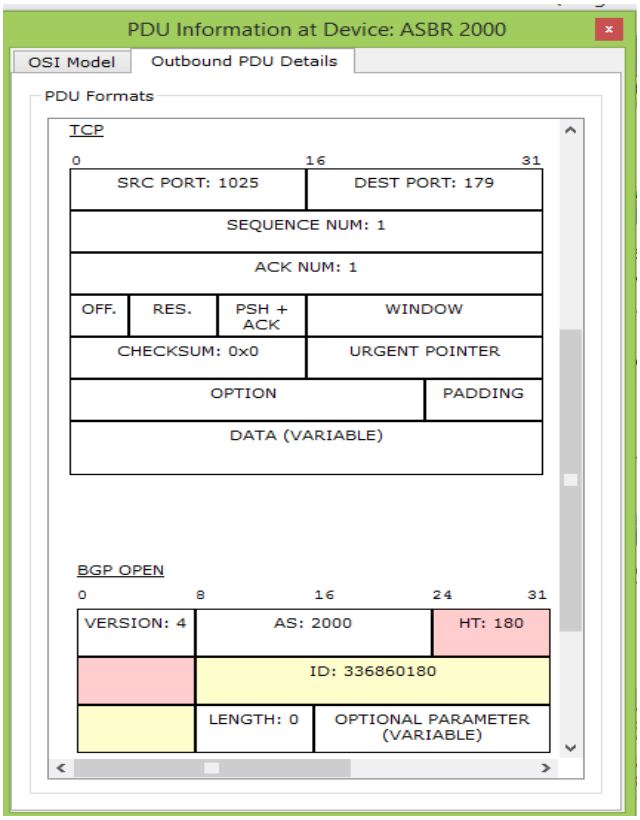


Fig. VII.18 Detalles del contenido del paquete BGP dentro del TCP.

Posteriormente, se normalizan los mensajes entre el AS 1000 y AS2000 y entonces, se recibe un paquete BGP KEEPALIVE, como se indica en la figura VII.19; mientras que los detalles de ese paquete se muestran en la figura VII.20.

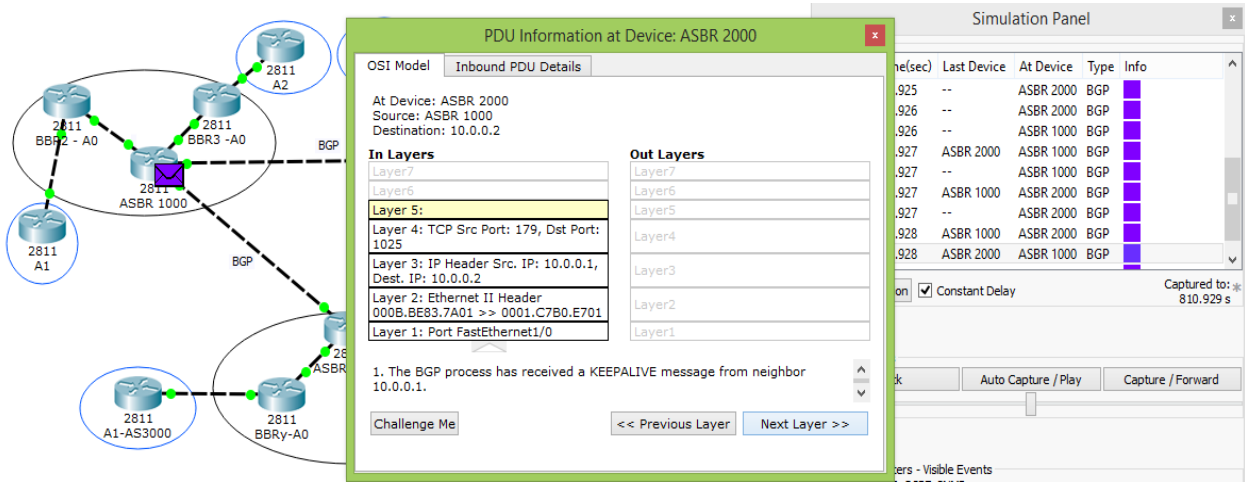


Fig. VII.19 Paquetes BGP OPEN y BGP KEEPALIVE entre los routers "ASBR 1000" y "ASBR 2000".

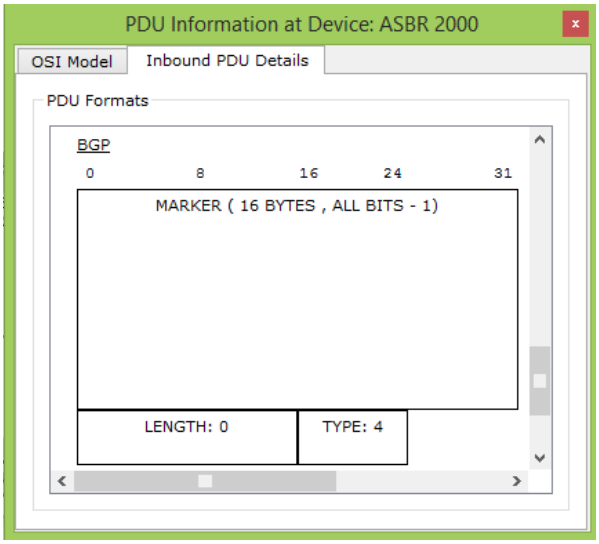


Fig. VII.20 Detalles del contenido del paquete BGP KEEPALIVE.

Por su parte, la configuración para el *router* "ASBR 3000" (*Autonomous System Backbone Router*) se muestra en la figura VII.21 y se observa cómo se levantan los enlaces BGP vecinos. Para reforzar la comprensión, es recomendable comparar con la configuración realizada en el *router* "ASBR 1000" (*Autonomous System Backbone Router*) indicada con antelación.

```
Router(config)#
Router(config)#router bgp 3000
Router(config-router)#bgp router-id 30.30.30.30
Router(config-router)#neighbor  20.0.0.1 remote-as 2000
Router(config-router)#neighbor  30.0.0.2 remote-as 1000
Router(config-router)#%BGP-5-ADJCHANGE: neighbor 20.0.0.1 Up
%BGP-5-ADJCHANGE: neighbor 30.0.0.2 Up
```

Fig. VII.21 Configuración del *router* ASBR 3000.

Una vez que existe conectividad total entre los tres sistemas autónomos, se pueden visualizar los paquetes BGP entre los ASBR1000, ASBR 2000 y ASBR 3000, cómo se indica en la figura VII.22. Obsérvese también la comunicación entre las capas de 1 a 4.

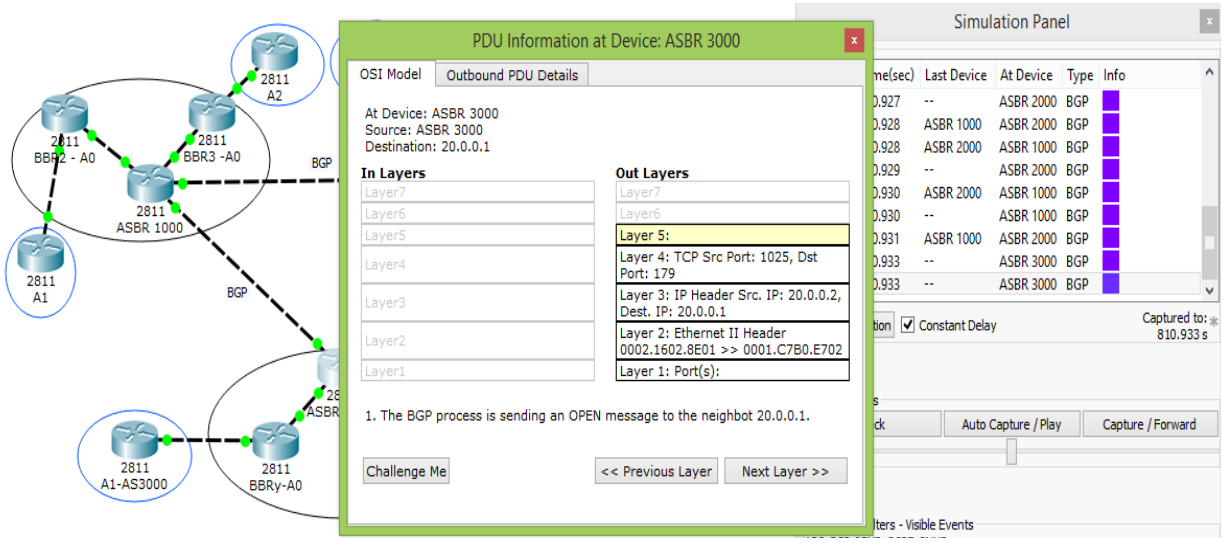


Fig. VII.22 Paquetes BGP OPEN y BGP KEEPALIVE entre los ASBR 1000 y 2000.

Una vez configurados los tres ASBR (*Autonomous System Backbone Router*), se obtiene una comunicación total mediante el intercambio de paquetes BGP, como se indica en la figura VII.23, con lo cual existe plena comunicación entre los tres sistemas autónomos.

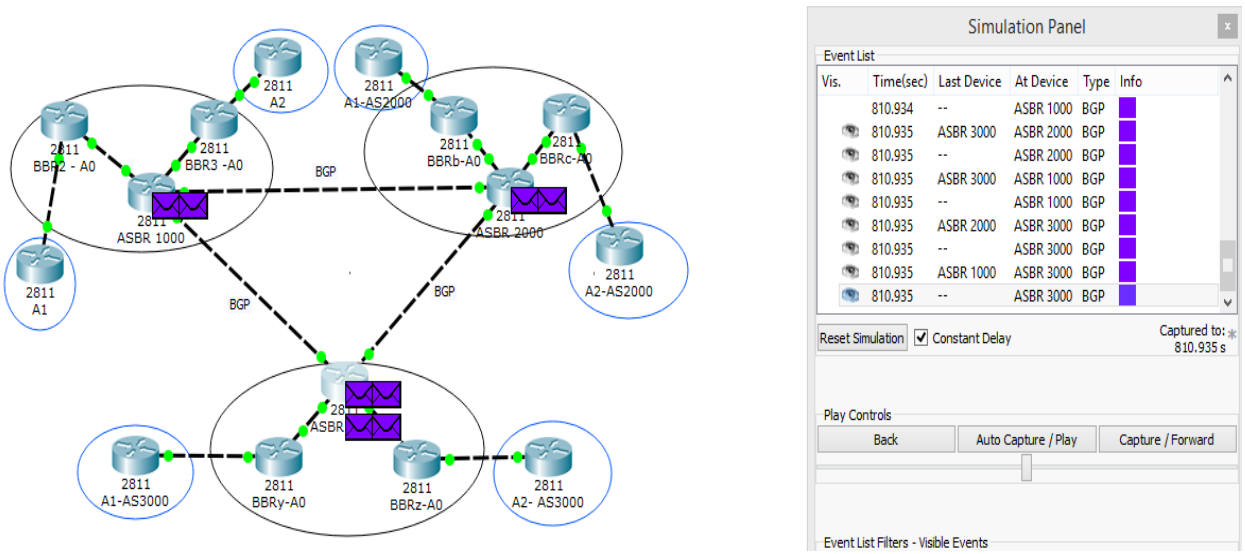


Fig. VII.23 Comunicación total bajo el protocolo BGP entre los distintos ASBR.

Con la finalidad de observar si se han llenado las tablas de enrutamiento, en las que se incluyen a las rutas creadas por BGP, se usa la orden, indicado en la figura VII.24, "*Show ip bgp*", de modo que se ha solicitado después de pedir la tabla de enrutamiento general, donde se observan las adyacencias indicadas mediante la letra "c", que señala las redes contiguas. Observe que la tabla no muestra que existan rutas conocidas mediante BGP.

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

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet1/0
C    30.0.0.0/8 is directly connected, FastEthernet1/1
Router>sh ip bgp
BGP table version is 3, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path

Router>
```

Fig. VII.24 Tablas de enrutamiento para el ASBR 1000.

Una vez que se configuró la redistribución de rutas, se irán llenando las tablas, al irse descubriendo las redes dentro de cada AS, y se compartira la información BGP entre todos los AS, respecto de las redes existentes en otros AS. En la figura VII.25, se muestra cómo se han compartido paquetes BGP y se van llenando las tablas de enrutamiento del *router* ASSBR 2000.

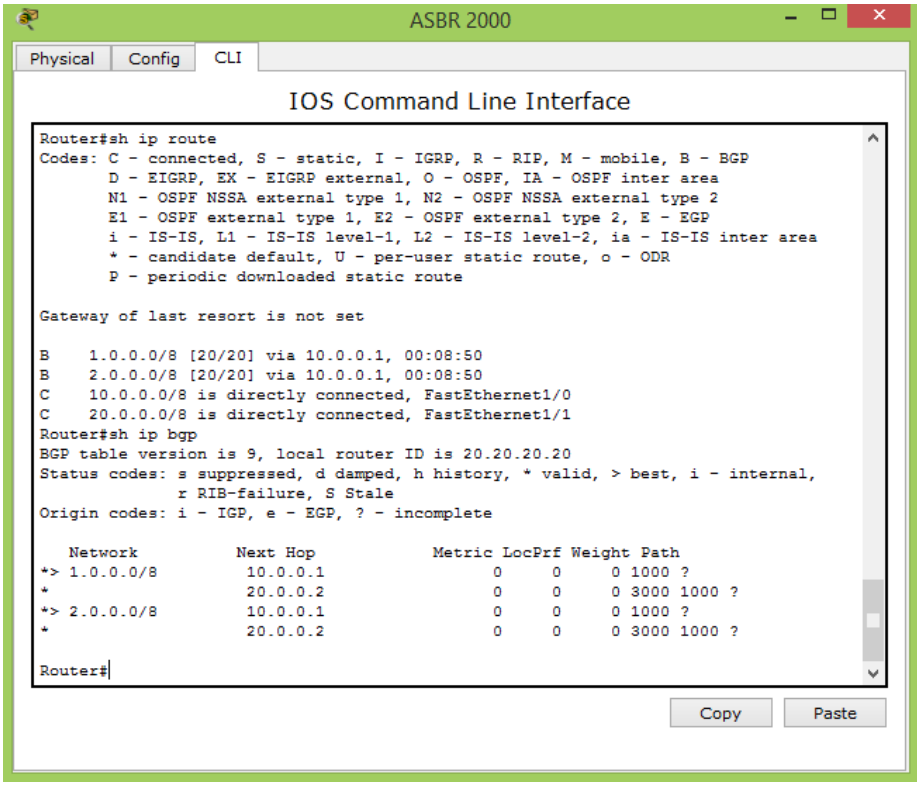


Fig. VII.25 Tablas de enrutamiento para el ASBR 2000.

En la figura VII.26, se muestra cómo se han compartido paquetes BGP y se van llenando las tablas de enrutamiento del *router* ASBR 3000.

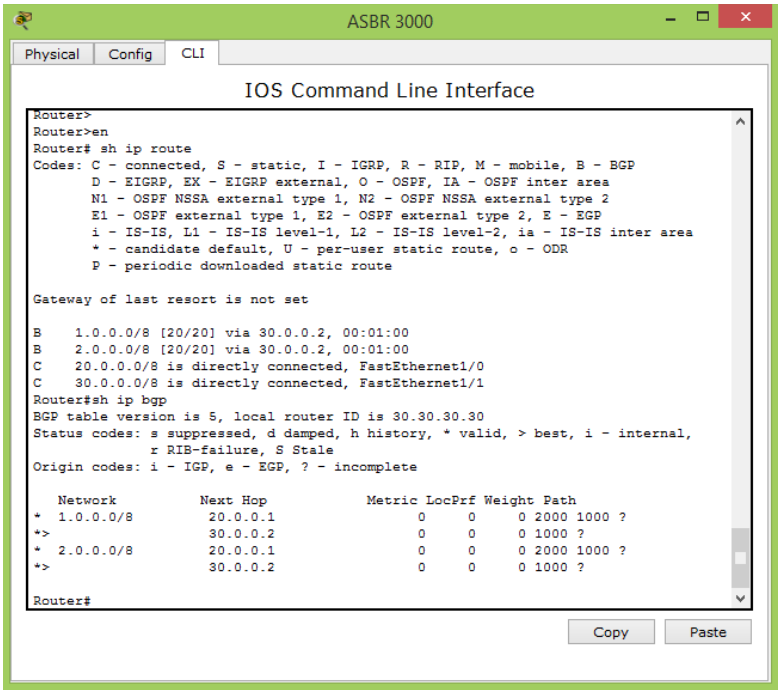


Fig. VII.26 Tablas de enrutamiento para el ASBR 3000.

VII.9.2 Evolución de BGP

La evolución de BGP se ha dado como se indica en la tabla VII.3. El BGP tiene su fundamento en el RFC 904 "*Exterior Gateway Protocol Formal Specification*", de 1984, y las evoluciones se dan con BGPv1, BGPv2, BGPv3 y BGPv4 **[71-74]**. Para el caso del RFC 2549, se usaron características que expandían BGP a IPv6 **[75]**.

Proposed Standard	*Draft Standard*	*Internet Standard*
BGP v1		
RFC 1105-1989 (experimental)		
BGP v2		
RFC 1163-1990 (historic)		
BGP v3		
RFC 1267-1991 & RFC 1268-1991		
BGP v4		
RFC 1654-1994 & RFC 1655-1994	RFC 1771-1995	
BGP-MP RFC 2545-1999 (Use of bgp-4 MultiProtocol extensions for IPv6 inter-do main routing)	**RFC 4271-2006**	

Tabla VII.3 *Routers* para el BB de CUDI o I2 en México desde 1999 hasta 2007.

A continuación, se aborda el caso de una red avanzada, que se resuelve con BGP, a la cual le llamo AMERONET, por ser la red que une las tres redes de América en una sola red.

VII.10 América

La unión de las 3 grandes redes avanzadas regionales (CANARIE, Internet 2 y CLARA) implica diferencias tecnológicas, principalmente en sus equipos y anchos de banda. La figura VII.27 muestra la topología de backbone en el continente americano, a la que, para abreviar, llamaremos la red AMERONET. En ella, se muestran los correspondientes anchos de banda para cada región. Se puede observar que hay 58 *routers* de *backbone* (25 en CANARIE, 15 en Internet 2 y 13 en CLARA), adicionalmente otros 5 *routers* de *backbone,* para realizar las conexiones entre AS, funcionando como ASBR y, finalmente, 15 *routers* de acceso, para un total de 73 routers [76].

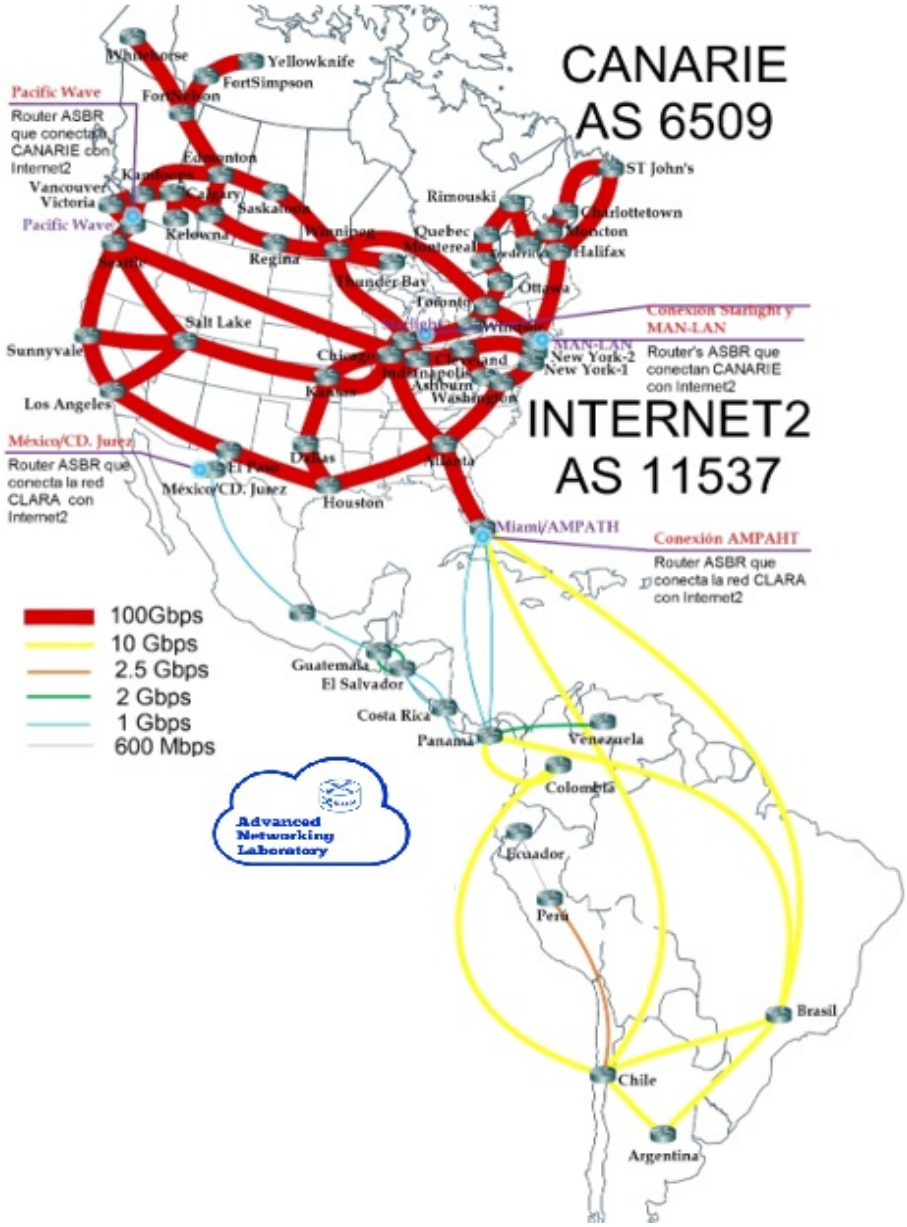


Fig. VII.27. Topología del *backbone* de las redes avanzadas de América.

Para realizar la simulación del funcionamiento de AMERONET, con *Packet Tracer,* se require solamente un equipo Core i3 con 4GB de RAM y la simulación ocupa casi el 30% del CPU y 45% de la RAM, para una ejecución de aproximadamente 3 minutos. La figura VII.28 muestra la simulación, indicando trayectorias de ida y vuelta al probar la conectividad de extremo a extremo, en la que se indican los paquetes ICMP [76].

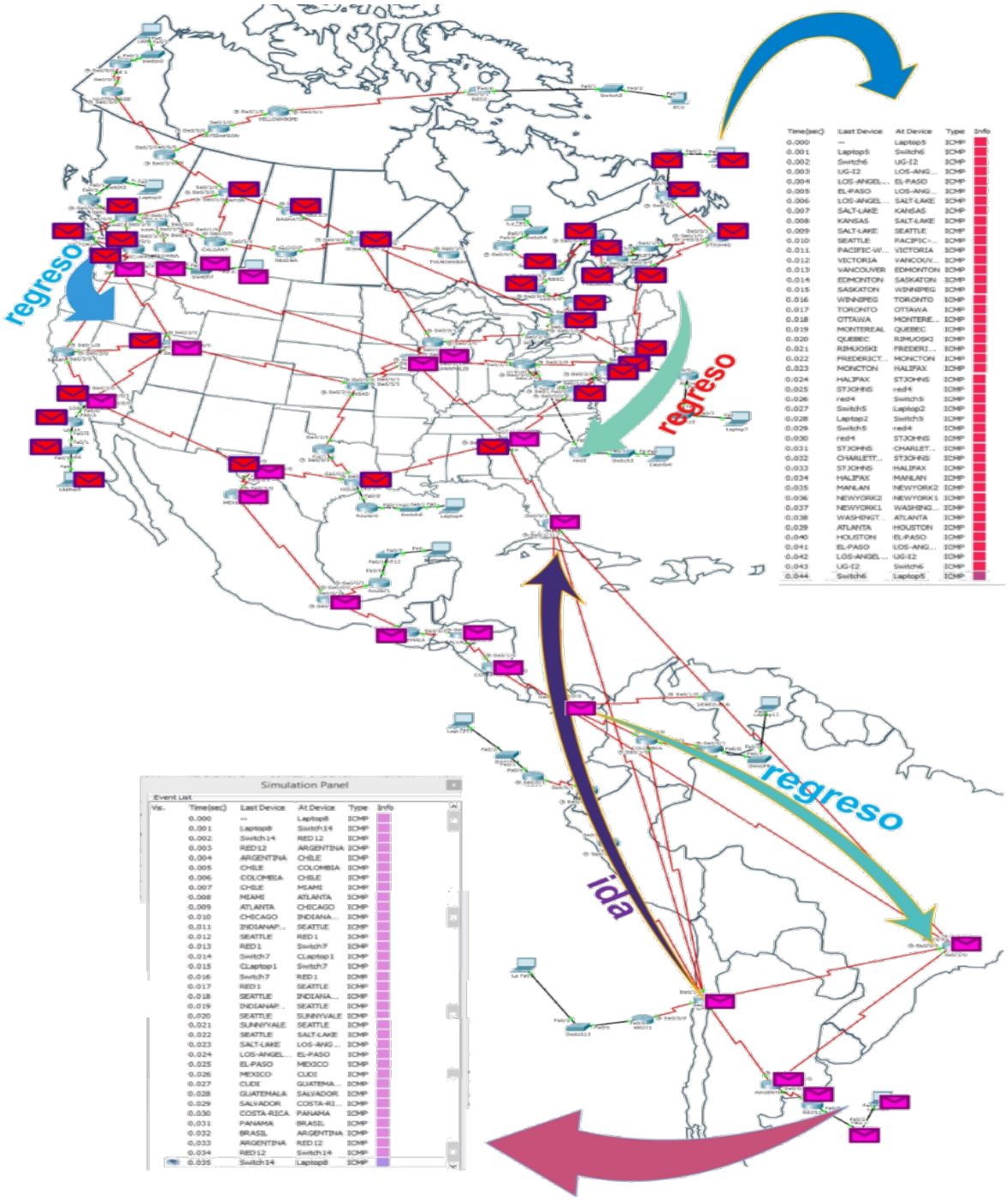


Fig. VII.28. Simulación de la topología del *backbone* de AMERONET.

La figura VII.29 muestra la topología de backbone de AMERONET, tal como se ha hecho la emulación en GNS3, usando los IOS de los equipos reales. Para el caso de la emulación en GNS3, es importante aclarar que ésta requiere de un procesador Intel Xeon (R) CPU E5-2620v2, a 2.10Ghz, con 12 núcleos y 24 procesadores lógicos y una memoria RAM de 32GB. La emulación completa, toma casi 37 minutos para estabilizar el encendido de todos los *routers* de *backbone* y consume casi el 80% de la RAM, así como el 30% del CPU; mientras que la conectividad, de extremo a extremo, se ejecuta en tiempo real con una latencia de casi 50ms [76].

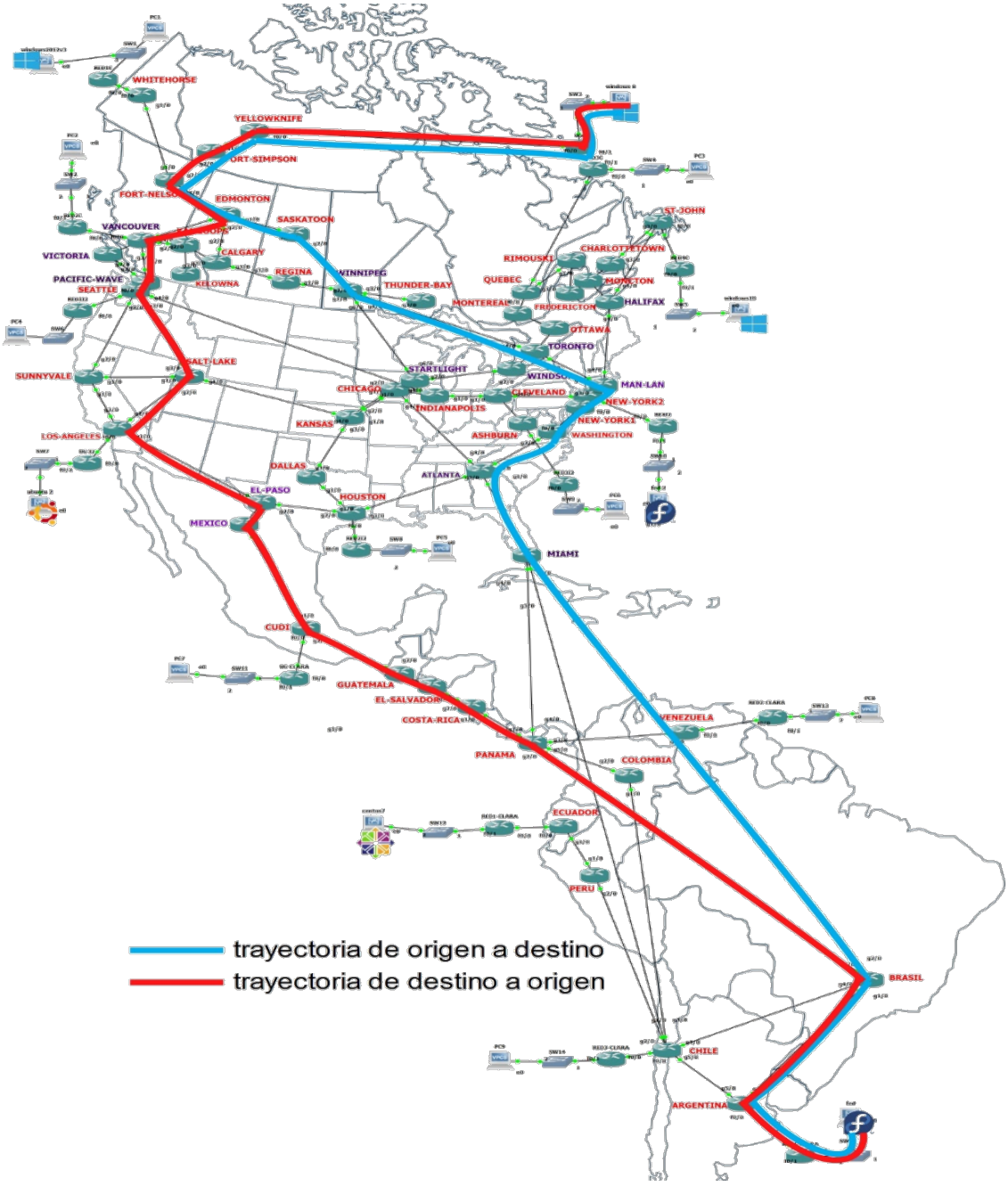


Fig. VII.29. Emulación de la topología del *backbone* de AMERONET.

VII.11 PRÁCTICA 8: Redes avanzadas

El objetivo es que el lector practique, mediante la simulación y la emulación, la conectividad y gestión aplicadas a la complejidad de las redes avanzadas.

Actividad 1: Elija alguna de las topologías de redes avanzadas, para simular y emular, de modo que compruebe la conectividad total y gestione, con base en el protocolo IPv4, todos los *routers*. Realice 5 pruebas de conectividad y gestión, desde una de las computadoras, que el lector elija, para que haga las veces de NMS.

Actividad 2: Simule y emule la red AMERONET, de modo que compruebe la conectividad total y gestione, con base en el protocolo IPv4, todos los *routers*. Realice 5 pruebas de conectividad y gestión, desde una de las computadoras, que usted elija, para que haga las veces de NMS.

CAPÍTULO VIII: PROTOCOLO IPV6

En 1981, cuando se publicó el IPv4, se creía que nunca se ocuparían los 4,300 millones de direcciones IP, que eso sería tanto como el infinito, pero al demandarse conexiones comerciales, entre 1990 y 1991, inició un crecimiento exponencial en el mundo, lo que llevó a la pregunta: ¿qué pasaría si los 7,000 millones de humanos tuvieran una conexión a Internet? En ese momento, las 4,300 millones de direcciones IP dejaron de parecer infinitas, por lo que se buscaron modos de extender las direcciones. Entonces, se propuso IPv6, para proveer casi 8 $x10^{28}$ veces la capacidad que ofrece IPv4, y es que IPv6 provee 3.4 $x10^{38}$ direcciones IP, hoy eso se parece un poco más al infinito.

VIII.1 Limitaciones de IPv4

En 1981 la Internet *Engineering Task Force* (IETF) liberó el IPv4, protocolo que permitía con sus direcciones de 32 bits, un total de 4.3 mil millones ($4.3x10^9$) de direcciones IP. La mayoría de los usuarios, alrededor del mundo, continúa usando el protocolo IPv4, ya sea para configurar tarjetas de red alámbricas o inalámbricas, así como para la asignación de redes y subredes. Sin embargo, al verse el incremento exponencial en el uso de Internet y, por lo tanto, del número de direcciones IP, se inició el desarrollo del protocolo IPv6. Como una medida, para extender el uso de IPv4, fue que se inventaron las subredes; pese a ello no fue posible extender más el uso de IPV4 **[77]**.

Las direcciones IPv6 son de 128 bits, o 16 bytes ($2^{128} \sim 3.4x10^{38}$ direcciones), en contraste con las direcciones IPv4, las cuales son de 32 bits o 4 bytes. Además, lPv6 usa el recurso de autentificación y acceso en DNS, para mapear los nombres de los hosts a direcciones IP, para lo cual también requieren soportar IPSec. La clave de cómo deben usarse las direcciones de IPv6 se encuentran en la arquitectura de direcciones de IPv6 **[78]**. Desde 1996, se usó la Internet 2 para continuar desarrollando al protocolo IPv6.

Para el año 2011, 16 años después de la liberación de IPv6, menos del 1% de los usuarios lo había implementado, habiendo más de 2 mil millones de usuarios en la Internet, un número inferior a la máxima capacidad de IPv4 de 4.3 mil millones de direcciones IP. Sin embargo, la APNIC (*Asia-Pacific Network Information Centre* – Centro de información de la red Asia Pacífico), uno de los 5 RIR (*Regional Internet Registries* - Registro Regional de Internet), casi había agotado todas sus direcciones IPv4 ese mismo año **[79]**.

Recordemos que un RIR es aquella organización que asigna y registra bloques de recursos de números de Internet (direcciones IPv4, direcciones IPv6 y números AS), tanto a los ISP como a otras organizaciones relevantes dentro de su región geográfica a la que da servicio. En este punto, cabe recordar que la versión IPv6 se implementó, a manera de prueba, globalmente el 6 de junio de 2012 en los principales ISP del mundo de manera simultánea. Desde ese momento, se ha venido incrementando el uso del protocolo IPv6 en las redes dorsales de la infraestructura de los propios ISP. Diríjase a la liga siguiente para ver el breve resumen alusivo a tan importante fecha, la cual marcó un hito en la historia de la Internet. El video se denomina *The new, larger version of the Internet: IPv6*, en el cual, Vinton Cerf, uno de los arquitectos de la Internet, da un didáctico resumen del desarrollo e implementación de IPV6. https://www.youtube.com/watch?v=-Uwjt32NvVA

De manera general, al comparar IPv6 contra IPv4, consideremos al menos 3 ventajas de IPv6:

a) IPv6 emplea un formato de paquete simplificado, para minimizar el procesado de encabezados por parte de los *routers*. Sin embargo, esto también hace que ambos protocolos no sean interoperables.
b) En IPv6 es mandatorio emplear seguridad, lo cual en IPv4 era opcional.
c) IPv6 permite que un host se autoconfigure al conectarse a una red IPv6.

Sin embargo, en este periodo de transición entre IPv4 e IPv6 en el que ambos conviven, se emplean ambas arquitecturas. Por lo tanto, en términos de seguridad siguen encontrándose algunos retos, ya que, por ejemplo, los firewalls deben crear 2 conjuntos de reglas para ambos tipos de tráficos. Y, mientras existe esa transición de IPv4 a IPv6, las organizaciones usan dos métodos de traducción entre ambos protocolos: el tunelamiento y la conmutación por etiquetas multiprotocolo. Sin embargo, ambos procesos implican de manera inherente alguna vulnerabilidad. Por ejemplo, cuando los usuarios hacen tunelamiento de tráfico desde redes IPv6 a IPv4, se usan redes privadas virtuales (*Virtual Private Networks* - VPN), aunque parecen seguras, también pueden tener problemas de seguridad o acceso a datos no autorizados. Una vez que tenemos claro las limitaciones de IPv4, a continuación, veremos en qué consiste IPv6 y cómo configurar *end systems*, servidores y *routers* con direcciones IPv6.

VIII.2 La habilitación del ISP para usar IPv6

La típica pregunta, que le surge a los administradores de una red, es: ¿Cómo puedo probar si mi red está habilitada para usar IPv6? La figura VIII.1 muestra una prueba, realizada desde una red LAN residencial, tal que (a) corresponde al caso de no tener habilitado IPV6 y (b) cuando se ha habilitado la infraestructura para IPv6. Identifique cada una de las características de la prueba [80].

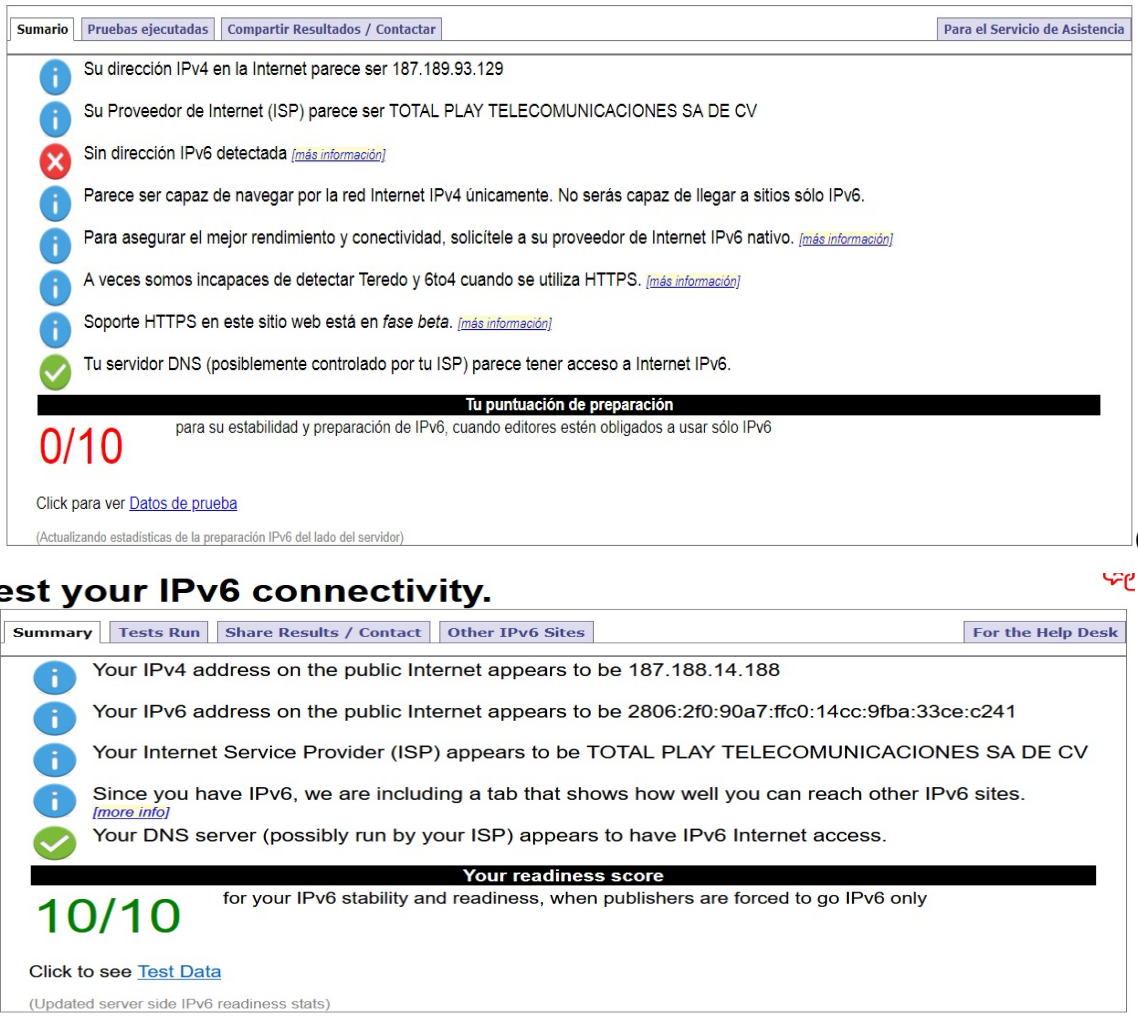


Fig. VIII.1. Prueba de conectividad para IPv6, (a) sin habitación, (b) con habilitación.

Cuando un usuario llega a tener habilitado IPv6, pero está usando un túnel público, o está mal funcionando, o una ruta se ha desconectado, o no funciona de manera óptima, se dice que se tiene una "conexión IPv6 rota, ruta o usuario rotos". Este tipo de problemas se resuelve cuando el correspondiente ISP ofrece conectividad IPv6 nativa, de otra forma, se puede deshabilitar IPv6.

VIII.3 Grado de adopción de IPv6 en el mundo

A todas aquellas compañías proveedoras de Internet, así como gestores de políticas públicas y promotores de páginas web, así como administradores de redes corporativas, les es de interés saber qué tanto se va adoptando IPv6. Por ello, se muestra en la figura VIII.2, el grado de adopción global para IPv6. También es posible conocer en qué medida se ha ido adoptando en los diferentes países. La captura indica 2008, sin embargo, el 31 de diciembre de 2022, se llegó al 40.85% como también es posible verificar en el gráfico [81].

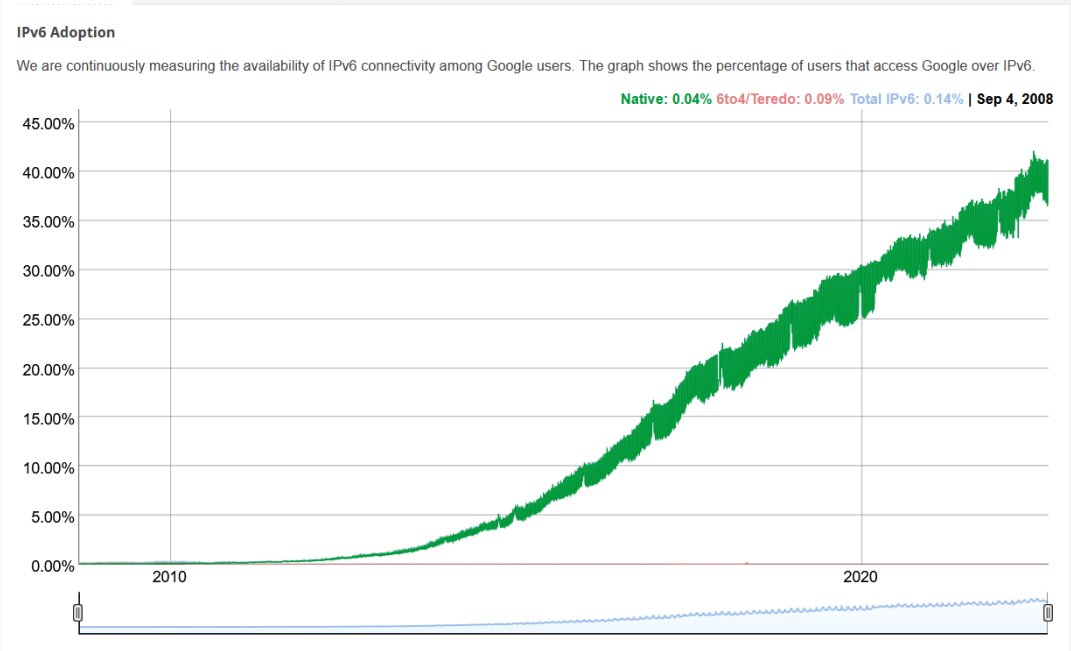


Fig. VIII.2. Adopción de IPv6 en el mundo desde 2008 a 2022.

La tabla VIII.1 muestra a los 20 países con mayor penetración de IPv6 en el mundo, hasta 2022 los cuales tienen una penetración superior al 20%, se trata del G20 de la IPv6 [81].

#	País	% adopción	#	País	% adopción
1	Francia	71.90	11	Taiwán	48.61
2	India	66.26	12	Japón	47.51
3	Alemania	64.98	13	EE. UU.	47.30
4	Bélgica	60.84	14	Hungría	45.
5	Malasia	59.54	15	**México**	**44.28**
6	Arabia Saudita	58.52	16	Reino Unido	44.13
7	Grecia	55.85	17	Tailandia	44.04
8	Vietnam	51.63	18	**Brasil**	**43.11**
9	**Uruguay**	**49.54**	19	Canadá	34.74
10	Finlandia	49.12	20	Portugal	32.03

Tabla VIII.1. Top 20 países en adopción de IPv6 (2022).

VIII.4 Protocolos para IPv6

A continuación, tenemos un ejemplo de una dirección IPv6 [78]:

1a00:1970:400b:807::2019

Pero, ¿cómo debe construirse para los casos ***unicast*** o *multicast*? En este texto sólo abordaremos el caso *unicast*.

Considérese que a diferencia de IPV4, en IPv6 se usan números hexadecimales (de preferencia en minúsculas) y se hacen 8 grupos de 4 dígitos decimales. Veamos un caso completo:

1234 : 5678 : 9abc : def0 : 0fed : cba9 : 8765 : 4321

Observamos que tupla hexadecimal grupo puede representarse por 16 bits, resultando en un total de 128 bits.

0001001000110100: 0101011001111000: 1001101010111100: 1101111011110000: 0000111111101101: 1100101110101001: 1000011101100101: 0100001100100001

A) ¿Cómo interpretar la dirección IPv6?

Suponiendo que la dirección anterior es una dirección tipo *unicast*, entonces los primeros 64 bits identifican el prefijo de red y la subred, en caso de existir; mientras que los otros 64 bits restantes son para indicar la interfaz de red de un host:

1234 : 5678 : 9abc : def0 : 0fed : cba9 : 8765 : 4321

Entonces:

B) La dirección de red

1234 : 5678 : 9abc : def0 : 0000 : 0000 : 0000 : 0000

Para lo cual existe una notación simplificada para el caso de las tuplas de ceros.

1234 : 5678 : 9abc : def0 : 0 : 0 : 0 : 0 Simplificación parcial para red

1234 : 5678 : 9abc : def0 :: Simplificación total para red

En este caso se indica completamente como:

1234678 : 9abc : def0 :: /64

C) Primera dirección para un host dentro de una red

1234 : 5678 : 9abc : def0 : 0000 : 0000 : 0000 : 0001

D) **Última dirección para un host dentro de una red**

1234 : 5678 : 9abc : def0 : ffff : ffff : ffff : ffff

E) Ejemplos de simplificaciones:

Si tenemos la dirección IPv6:

1234 : 5678 : 9ABC : 0000 : 0000 : CBA9 : 8765 : 4321 Dirección completa

1234 : 5678 : 9ABC :0: 0 : CBA9 : 8765 : 4321 Dirección parcialmente simplificada

1234 : 5678 : 9ABC :: CBA9 : 8765 : 4321 Dirección simplificada

F) Dirección de *loopback* IPv6

0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001 Dirección completa

0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 Dirección parcialmente simplificada

::1 o **::**1/128 Dirección simplificada

Recordemos que el término *Loopback* se refiere a la dirección *unicast* del *localhost*, que en IPv4 corresponde a la dirección 127.0.0.1; mientras que en IPv6 es ::1/128. Esto significa que, si una aplicación del host envía paquetes hacia esa dirección, entonces estos se enviarán de regreso sobre la misma interfaz virtual de salida.

G) Dirección indefinida o por defecto

En IPv4, la dirección por defecto es aquella que tiene todos sus bits en cero y no puede asignarse a interfaz alguna, ya que es la que usan las aplicaciones antes de conocer las direcciones de origen de una conexión; es decir, se está indicando que una aplicación está escuchando en toda interfaz disponible, por lo que en IPv6 se le llama indefinida.

0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 Dirección completa

0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Dirección parcialmente simplificada

::0 o **::**/128 Dirección simplificada

VIII.5 Protocolos de enrutamiento para IPv6

Después de RIP, se desarrolló el protocolo OSPF, cuya versión 1 nunca se implementó, pero si OSPFv2 [25]. Para 1999, se desarrolló OSPF para IPv6, conocido como OSPFv3, a través del RFC 2740 [82]. OSPF v3 fue actualizado por el RFC 5340, en 2009 [83].

A) ¿Qué se mantuvo sin cambios de OSPFv2 a OSPFv3?

Básicamente, los mecanismos fundamentales de OSPF: *Flooding*, la elección del Router designado (Designated Router - DR), el soporte de áreas, los cálculos del protocolo Primero el Camino Corto (*Short Path First* - SPF), entre otros. En la tabla VIII.2 se muestra el encabezado del paquete OSPF para IPv6, el cual consta de 16 bytes. Observe los grupos de 32 bits indicados en la parte superior de la tabla.

0	8	16	24 31
Version = 3	Type	Packet length	
Router ID			
Area ID			
Checksum		Instance ID	Must be cero

Tabla VIII.2. Encabezado del paquete OSPF IPv6.

Para el caso de la *Version,* ésta se indica con el número 3 y se mantienen los mismos 5 tipos de paquetes que en IPv4. Para el caso de *Instance ID*, se habilita la ejecución de varias instancias del protocolo OSPF sobre un mismo enlace.

B) Modificaciones al paquete OSPF *Hello*

El paquete *Hello* es de tipo 1 y se envía periódicamente sobre todas las interfaces, incluyendo las interfaces virtuales, con la finalidad de descubrir *routers* vecinos. La tabla VIII.3 muestra los campos relacionados con el paquete *Hello*, observe que los primeros 16 bytes corresponden al encabezado OSPFv3. Note también que el campo *options* se modificó, de 8 bits en OSPFv2 a 24 bits en OSPFv3.

0	8	16	24 31
3	1	Packet length	
Router ID			
Area ID			
Checksum		Instance ID	Must be cero
Interface ID			
Router Priority	Options		
Hello Interval		Router Dead Interval	
Designated Router ID			
Backup Designated Router ID			
Neighbor ID			

Tabla VIII.3. Paquete *Hello* de OSPF IPv6, incluyendo el encabezado en sombreado.

Donde:

Interface ID, es el número identifica a una interfaz entre una colección de interfaces de un *router*.

Router priority, si el valor se coloca en 0, entonces no será posible elegirlo DR.

Hello Interval, indica el número de segundos entre los paquetes *Hello* del *router*.

Router Dead Interval, se indica el número de segundos requeridos para declarar a un *router* apagado.

Designated Router ID, envía la vista de identificación del DR para la red. Solamente si se indica como 0.0.0.0 implica que no hay asignado un DR.

Backup Designated Router ID, el *router* que envía su identificación como BDR. Si se indica como 0.0.0.0 implica que no hay asignado un BDR.

Neighbor ID, es el identificador de *router* en la red con el estado de su vecino, inicia en uno o un número mayor.

C) Modificaciones al paquete DBD

En este caso se sigue usando para intercambiar paquetes entre *routers* que se están inicializando, para describir el contenido de la base de datos del enlace y también se pueden enviar varios paquetes para describir a las bases de datos. Para ello se usa el procedimiento encuesta-respuesta, además uno de los *routers* se designa como maestro y otro como esclavo.

0	8	16	24 31
3	2	Packet length	
Router ID			
Area ID			
Checksum		Instance ID	Must be cero
Must be cero	Options		
Interface MTU	Must be cero	0 0 0 0 0 I M MS	
DD Sequence Number			
An LSA Header			

Tabla VIII.4. Paquete DBD de OSPF IPv6, incluyendo el encabezado en sombreado.

Donde

Interface MTU, indica el tamaño en bytes del datagrama IPv6 más grande, que se puede enviar fuera de la interfaz asociada sin fragmentarla. Para hacer envíos sobre los enlaces virtuales, el valor debe ser cero.

Bit I, toma el valor de 1 cuando es el primer paquete en la secuencia de los paquetes del DBD.

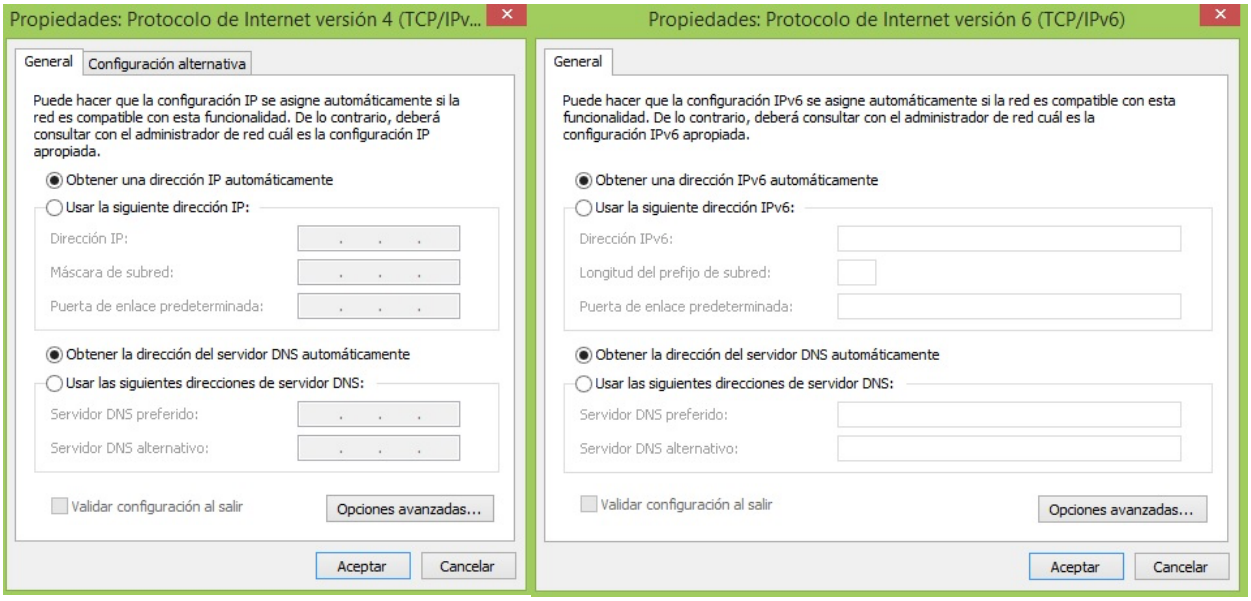
Bit M, toma el valor de 1 para indicar que hay más paquetes DBD asociados.

Bit MS, es el bit maestro esclavo; cuando se coloca en 1, indica que el *router* es el maestro durante el proceso, mientras que, con el valor de 0, indica que el *router* es el esclavo.

DD sequence number, se usa para dar secuencia a la colección de paquetes DBD. Este número se va incrementando, hasta que se completa la transferencia de la base de datos, para ambos *routers:* el maestro y el esclavo.

LSA header, consiste en una lista de las piezas de la base de datos del estado del enlace y contiene información requerida para identificar únicamente tanto al LSA como a la instancia actual del LSA.

En la figura VIII.3, se muestran las opciones para configurar una tarjeta GE, ya sea usando IPv4 o IPv6. Estas opciones se pueden hallar en la configuración de su propio equipo, en lo relativo a la opción para la configuración de IPv4 o IPv6 en la tarjeta de red Gbps, tanto para la NIC como para la WNIC. La figura VIII.3a corresponde a la configuración para IPv4, mientras que la figura VIII.3b corresponde a la configuración IPv6.



(a) (b)

Fig. VIII.3. Opciones de configuración en una NIC para IPv4 e IPv6.

VIII.6 Protocolos de gestión para IPv6

En 1990 surgió el protocolo SNMP v1, mediante el RFC 1157, y en 1992 se emitió el SNMP v2, vía los RFC de 1901 a 1908, mejorando la seguridad, usando cadenas de comunidad y el funcionamiento del protocolo, permitiendo recuperar informes de mensajes de error más detallados y masivos con "GETBULK". El protocolo SNMPV3, respaldado en los RFC 2263, RFC 2273 y RFC 2275, mejoró agregando autentificación y encriptación de paquetes, lo que provee los protocolos de seguridad DES/AES, para que la comunidad sea encriptada mediante los algoritmos MD5 o SHA. **[84-86]**. Las versiones más recientes de SNMPv3 están en los RFC 3410 al 3415 **[87, 88]**. SNMPv3 agregó cinco operaciones y la descripción de ellas se indica en la tabla VIII.5. En el apartado de criptografía, se abordarán brevemente DES/AES, MD5 y SHA.

Operación	Descripción
Get-request	Lee el valor de una variable específica.
Get-bulk-request	Lee grandes bloques de datos, provenientes de varias filas en una tabla, así se evita la transmisión de muchos bloques pequeños de datos.
Set-request	Escribe un valor en una variable específica.
Get-response	Responde a una operación get-request, *get-next-request* y *set-request* que envió el NMS.
Get-next-request	Lee el valor de una variable solicitada, dentro de una tabla, de modo que el administrador de SNMP no necesita saber el nombre exacto de la variable; razón por la que realiza una búsqueda secuencial.

Tabla VIII.5. Operaciones de SNMPv3.

El sistema de gestión de red podría controlar el uso de CPU de un *router* entre otros parámetros. Básicamente, para el control de la actividad en la red, se usan dos métodos: por encuesta o por alarmas. El control de actividad por encuesta consiste en que el administrador debe hacer explícitamente la consulta, sin embargo, hay dos desventajas con este método: Una es el retraso entre la ocurrencia de un evento y el momento en el que el sistema de gestión de red puede percatarse; y la otra desventaja es que debe haber un equilibrio entre la frecuencia con la que se hacen las encuestas y el uso del ancho de banda, ya que hacer encuestas de manera muy frecuente

disminuye el desempeño del ancho de banda. Por su parte, el método de alarmas o *traps*, permite que un agente SNMP genere y envíe un tipo de alarma automáticamente cuando ocurre un evento para así informar de inmediato al sistema de gestión.

VIII.7 Fundamentos de criptografía

La criptografía muchas veces es considerada ajena al trabajo diario y apenas percibida sólo cuando la gente necesita realizar transacciones bancarias. Sin embargo, se usa no sólo a diario sino a cada momento, prácticamente, cada vez que usamos una computadora. Recuerde que un teléfono celular actual es una computadora, así como los equipos de telecomunicaciones, todos son computadoras para aplicaciones específicas. Todas las aplicaciones de software, para las VPN cliente servidor, usan criptografía simétrica, asimétrica e híbrida. La criptografía se puede aplicar en distintos niveles, considerando el modelo TCP/IP, desde la capa 1 hasta la capa 5.

Algoritmos Criptográficos

Tanto para servidores como para *routers* y *firewalls* y todo dispositivo relacionado con la seguridad, se requiere garantizar la seguridad y la privacidad de la información, la cual queda definida por la confiabilidad, integridad y disponibilidad de la información. Para ello se usan distintos algoritmos de encriptación en los diferentes niveles, ya sean mecanismos de seguridad de capas inferiores o de capas superiores. En el caso de los algoritmos de encriptación, podemos encontrar el estándar de encriptación de datos (*Data Encryption Standard* – DES) y el estándar de encriptación avanzada (*Advanced Encryption Standard* - AES), con sus diferentes variantes, para el uso de *hashing* o cadenas MD5 y SHA; mientras que para autenticación se puede encontrar RSA en modalidad de llaves, encriptación y firmas. A continuación, se abordan brevemente cada uno de ellos.

Cifrados simétricos, asimétricos e híbridos

A) **DES** es un algoritmo de cifrado, liberado en 1976, el cual tiene un tamaño de clave de 64 bits, mientras que para la parte criptográfica se usan 56 bits. Pese a sus mejoras, como 3DES, en 1998, DES fue violado y declarado inseguro, de modo que en la actualidad no debe ser usado solo, sino en combinación con otros algoritmos **[89]**. Desde 2002 AES lo sustituye para la mayoría de las aplicaciones.

B) **AES** es un algoritmo de cifrado de bloques simétrico que puede procesar bloques de datos de 128 bits, para lo cual usa llaves de 128, 192 y 256 bits (en tales casos se les conocen como AES-128, AES-192 y AES-256), el cual fue convertido a estándar en 2002. Existen algunas evidencias de que AES de 128 y AES de 192 bits, ya fueron violados criptográficamente **[90]**.

A la fecha no hay evidencia pública de que AES de 256 haya sido violado criptográficamente por lo que es el que siguen usando los bancos y las agencias de gobierno.

AES es una de las criptografías más usadas en *routers*, y para VPN: se usa en Open VPN e IPSec, ya que estos emplean bibliotecas OpenSSL. Tanto a Open SSL como a Libre SSL, se les conoce como bibliotecas criptográficas. Con base en ellos, se obtienen variantes AES, tales como: AES-CBC (Cipher - Block Chaining), AES-CFB (Cipher Feedback) y AES-OFB (Output Feedback) **[91]**.

Una aplicación específica que usa estos cifrados, puede ser BitTorrent, muy usado para el intercambio de archivos grandes, punto a punto. Es tan popular que es responsable de casi el 40% del tráfico de internet, uno de sus servicios incluye el uso de VPN **[92]**.

C) **RSA** (Rivest-Shamir-Adleman) es un algoritmo de cifrado de bloques asimétrico, creado en 1977 y patentado en 1983, pero la patente expiró en el año 2000, por tanto, se ha hecho público. RSA realiza 3 funciones: generación de claves, cifrado y descifrado, para lo cual usa dos números primos aleatorios y genera 2 claves, una pública y una privada. Actualmente, por seguridad, se recomienda usar RSA con claves de 4096 bits **[93]**.

Funciones criptográficas *Hash* o de resumen

Una función *hash* permite crear el equivalente a la huella digital única de un archivo, la cual le permite desde el lado de emisor y receptor en una transmisión saber si se ha corrompido o no, para lo cual usa un tipo de cifrado. Básicamente tiene tres funciones: identificar que un archivo no se haya modificado durante su transmisión; hacer ilegible una contraseña o permitir firmar digitalmente un documento. Es decir, su entrada es un texto o imagen y su salida es una cadena de caracteres de longitud fija. Los dos sistemas criptográficos más populares son el algoritmo de resumen de mensajes 5 (*Message Digest Algorithm* 5 - MD5) y el Algoritmo de "hash" o cadena segura (*Secure Hash Algorithm* - SHA-3).

D) **MD5** es un algoritmo de reducción de 128 bits, que prueba la integridad de mensajes, el cual fue diseñado para máquinas de 32 bits y sustituyó, en 1991, al MD4, que era más rápido que el MD5, pero menos robusto en seguridad; éste, a su vez, sustituyó al MD3, quien, a su vez, reemplazo al MD2 y éste al MD 92 de 1992 **[94]**. En la actualidad todos los MD han sido violados. Una aplicación que nos permita ver en ejecución las funciones criptográficas, la

podemos obtener en alguna distribución del sistema operativo Linux, como se indica en la tabla VIII.6, en la que podemos apreciar: a) el cifrado de un texto y b) la huella de un archivo, aun cuando también se puede emplear para cifrar contraseñas. Observe, en la salida los 128 bits o 32 dígitos hexadecimales.

E) SHA es un algoritmo de cadenas similar a los algoritmos MD. Después de SHA-0, SHA-1, SHA-2, la última versión es la SHA-3. Por ejemplo, SHA-1 tiene 160 bits, es más seguro que MD5, pero más lento. Por su parte SHA-2 llega a los 512 bits. En este caso, en Linux la orden a usar es "sha1sum". Para Windows puede probar "*Snap MD5"*.

La tabla VIII.6 muestra transformaciones mediante la función de resumen MD5.

Linux:~$ **md5sum**
.....TEXTO
Linux:~$ **md5sum**
ADVNETLAB
3hzgsxy292ts91js9849437a738j2w3fu -
….....ARCHIVO
Linux:~$ **md5sum** foto1.jpg
Abcd3hzgs437a738js91js98491u3h47 foto1.jpg
.....FIRMA DIGITAL
Linux:~$ **gpg clearsign** foto1.jpg
Password for unlooking "secret password"
User xyz (Public key)
< aurum@advnetlab; quot;
Key DSA 4040 bits, ID BFAD1618, created 2022-10-10

Tabla VIII.6. Uso de la función MD5.

Aplicaciones que incluyen criptografía para VPN

Una de las aplicaciones que usa criptografía para permitir la creación de una red privada virtual (*Virtual Private Network* - VPN) es el navegador Opera, el cual es considerado uno de los más seguros y que menos energía consume. La figura VIII.4, muestra el anuncio de esa característica. Se recomienda al lector instalarlo y habilitar la funcionalidad VPN.

Fig. VIII.4. Mensaje sobre la funcionalidad criptográfica al instalar Opera.

Otros casos de uso cotidiano de la criptografía se dan en aplicaciones, que se usaban bajo un modelo de negocio tradicional y que ahora usan computación en la nube, bajo el modelo Software como un servicio (*Software as a Service* - SaaS), por ejemplo, Office 360 de Microsoft, el cual desde el año 2013 se ofrece como SaaS y se cobra bajo suscripciones anuales.

Entonces, ¿qué sucede si adquirimos una suscripción de Office y dejamos de pagarla? Office se puede seguir usando, no se desinstala, los archivos pueden seguirse visualizando, lo que queda desactivada es la posibilidad de editar archivos. Por tanto, cuando se paga nuevamente la suscripción, se habilita la edición. Entonces, de alguna manera, la encriptación está en la transmisión de datos y al compartir claves con caducidad. Ello tiene importantes implicaciones para evitar la piratería, instalando las aplicaciones en una sola computadora sin opción para hacer instalaciones de una licencia en varios equipos **[95]**.

Paradigma de la criptografía cuántica

Dado que toda seguridad dentro del paradigma de la computación tradicional de la tercera revolución industrial es vulnerable, se ha desarrollado la computación cuántica, de modo que la seguridad vía los algoritmos cuánticos sea, en teoría, inviolable. Este paradigma de criptografía se está desarrollando a nivel de computadoras y también a nivel de transmisión de información vía satélite. En esta carrera tecnológica relativamente nueva, China lleva la delantera.

Con la finalidad de que tenga una mejor idea acerca del paradigma de la encriptación, con base en la computación cuántica, deben consultar el siguiente video: “Satélite cuántico chino logra comunicación a larga distancia - 2017”, https://www.youtube.com/watch?v=4QlcKuxDGrs

VIII.8 Túneles entre IPv4 e IPv6

Busquemos ahora responder a la pregunta: ¿Es posible comunicar directamente una computadora, cuya NIC se encuentra configurada con IPv4 y otra configurada con IPv6? Si usted intenta contestar auxiliándose de una simulación, encontrará que los paquetes generados de IPv4 a IPv6, serán descartados desde antes del envío del paquete ICMP, como se muestra en la figura VIII.5, de modo que no habrá comunicación entre ambas.

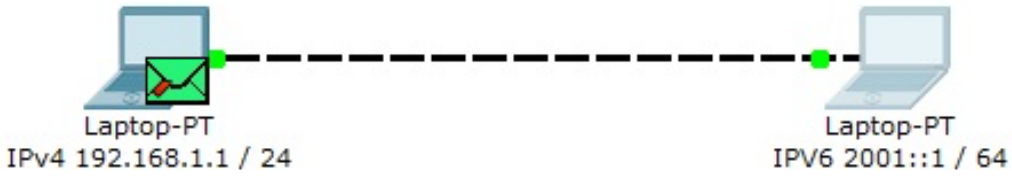


Fig. VIII.5 Intento de comunicación directa IPv4 a IPv6.

Entonces, para conectar 2 computadoras, una cuya NIC se haya configurado como IPv4 y otra como IPv6, se requiere tratarlas como si estuvieran conectadas en redes diferentes; por lo tanto, tendrán que pasar por *routers,* como se indica en la configuración básica de la figura VIII.6. Primero, configuramos a las NIC de las computadoras, como en el caso de una red IPv4, y probamos su conectividad.

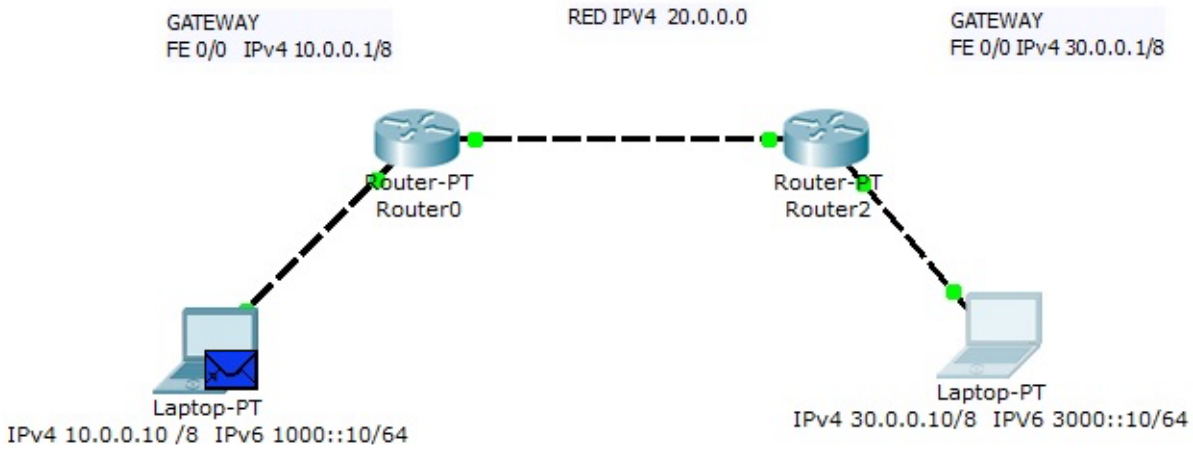
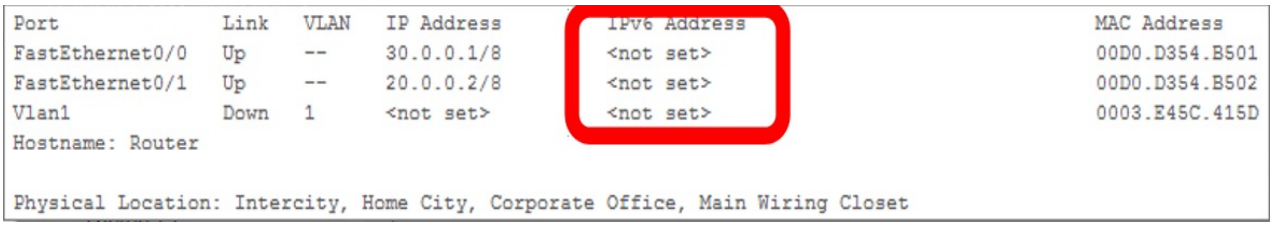


Fig. VIII.6 Comunicación directa IPv4 a IPv6.

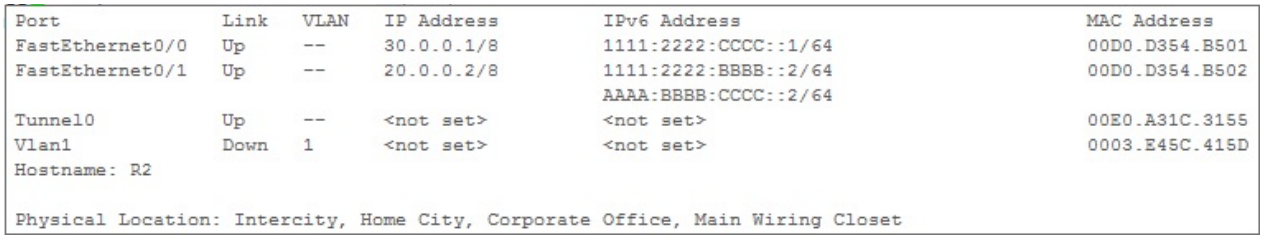
Debe corroborar que, mientras no se configure IPv6, no aparecen ni las direcciones con tal protocolo y tampoco la posibilidad de habilitar un túnel entre IPv4 e IPv6, como se indica en la figura VIII.7a en su parte superior; mientras que, en la figura VIII.7b, en su parte inferior, se muestra al mismo *router* con configuración IPv6 y es posible observar al túnel habilitado.



```
Port              Link   VLAN   IP Address        IPv6 Address                  MAC Address
FastEthernet0/0   Up     --     30.0.0.1/8        <not set>                     00D0.D354.B501
FastEthernet0/1   Up     --     20.0.0.2/8        <not set>                     00D0.D354.B502
Vlan1             Down   1      <not set>         <not set>                     0003.E45C.415D
Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

(a)



```
Port              Link   VLAN   IP Address        IPv6 Address                  MAC Address
FastEthernet0/0   Up     --     30.0.0.1/8        1111:2222:CCCC::1/64          00D0.D354.B501
FastEthernet0/1   Up     --     20.0.0.2/8        1111:2222:BBBB::2/64          00D0.D354.B502
                                                   AAAA:BBBB:CCCC::2/64
Tunnel0           Up     --     <not set>         <not set>                     00E0.A31C.3155
Vlan1             Down   1      <not set>         <not set>                     0003.E45C.415D
Hostname: R2

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

(b)

Fig. VIII.7 *Router* (a) antes y (b) después de configurarlo con IPv6.

Luego, creamos la misma red, pero configurada como una red IPv6, tal y como se indica, para el *router* R1, en la figura VIII.8.

```
Configuración en IPv6.
R1(config)#ipv6 unicast-routing
R1(config)#int fa0/0
R1(config-if)#ipv6 address 1111:2222:aaaa::1/64
R1(config-if)#exit
R1(config)#int fa0/1
R1(config-if)#ipv6 address aaaa:bbbb:cccc::1/64
R1(config-if)#ipv6 enable
R1(config)#interface tunnel 0
R1(config)#tunnel source fa0/1
R1(config)#tunnel destination 20.0.0.2
R1(config)#tunnel destination 20.0.0.2
R1(config)#ipv6 route 1111:2222:cccc::/64 aaaa:bbbb:cccc::2
```

Fig. VIII.8 Configuración en IPv6.

Analice:

a) ¿Cómo se habilita el enrutamiento IPv6 unicast para todo el *router?*
b) ¿Cómo se asignan direcciones IPv6 en las interfaces de cada *router*?
c) ¿Cómo se habilita IPv6 en la interfaz entre los *routers*?
d) ¿Cómo se crea una interfaz de túnel, en la que se especifican la interfaz origen y la destino como dirección IPv4 de la interfaz de R2?
e) ¿Cómo se configura una ruta estática IPv6 no contigua, indicando toda la red destino y la interfaz en R2 sobre la cual se alcanzará o a la que habrá que llegar primero?

Finalmente, después de configurar a los 2 hosts y a los 2 *routers*, se obtiene la topología de la red indicada en la figura VIII.9, en la cual se muestran todos los detalles de direcciones IPv4 e IPv6.

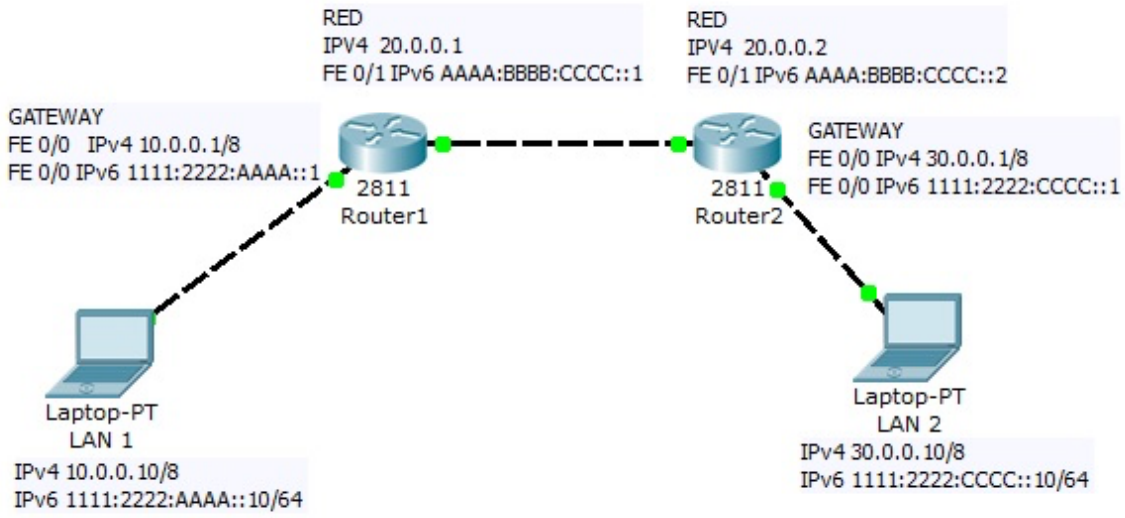


Fig. VIII.9 Topología para una red que permite tunelamiento entre IPv6 e IPv4.

En la figura VIII.10, observe cómo es que se envía un PDU complejo, para poder hacer el envío desde una dirección IPv6 a una dirección IPv4.

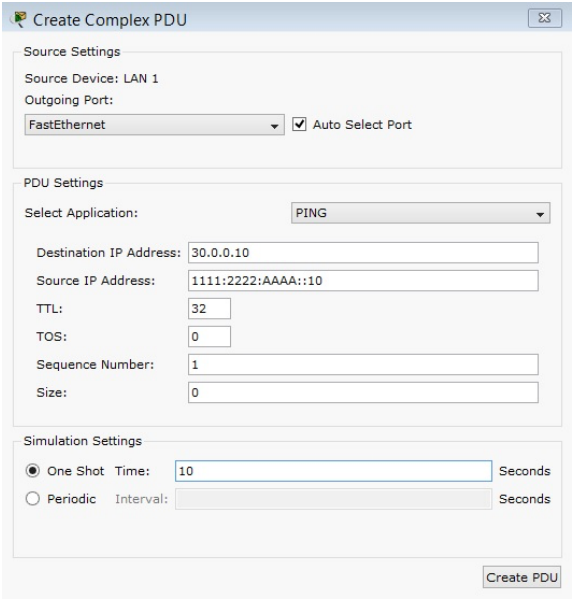


Fig. VIII.10 Envío de un ping desde un equipo con IPv6 hacia IPv4.

Durante la ejecución de la orden ping debe ser posible verificar que el paquete IP está enviándose en la capa 3 del modelo TCP/IP, desde la dirección IPv6 a la dirección IPv4, como se indica en los detalles del formato de paquete de la figura VIII.11.

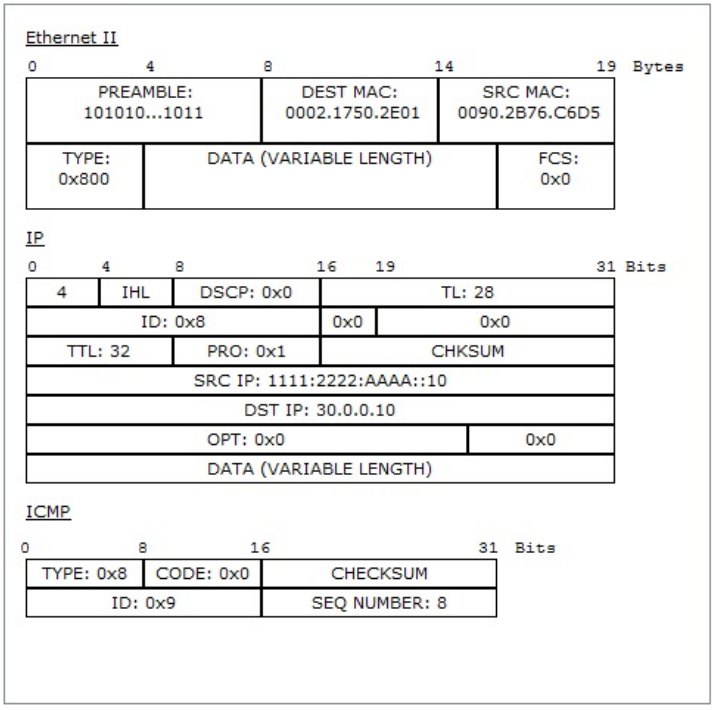


Fig. VIII.11. PDU el cual contiene trama, paquete IP e ICMP para comunicación IPv6 a IPv4

Finalmente, cuando el paquete ICMP llega al host destino, una vez que ha operado el tunel, es posible observar, en términos de las capas del modelo ISO/OSI, tanto el paquete que llega al host destino (izquierda), como el paquete que irá de regreso a la salida del host (derecha), tal y como se muestra en la figura VIII.12.

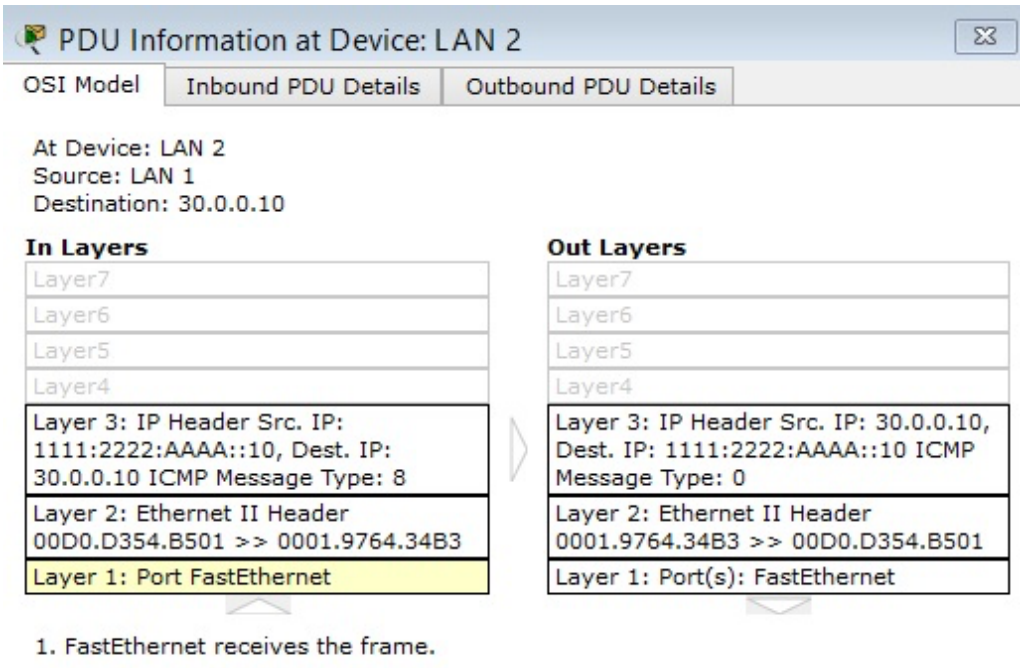


Fig. VIII.12 PDU que contiene trama, paquete IP e ICMP, para la comunicación de IPv6 a IPv4.

Con la finalidad de poder transmitir datos, es posible usar direcciones IPv6 sobre IPv4 **[96]**. Algunas direcciones usadas para el tunelamiento son:

::f f f f :0:0 / 96

pero también el prefijo:

64:f f 9 b:: / 96

VIII.9 Europa – África (Interconectando sistemas autónomos por BGP)

La figura VIII.13 muestra la emulación de la topología de backbone que resulta de unir GEANT con AFRICACONNECT para los dos continentes. En este caso la conectividad y la gestión se realizó bajo IPv6 [97].

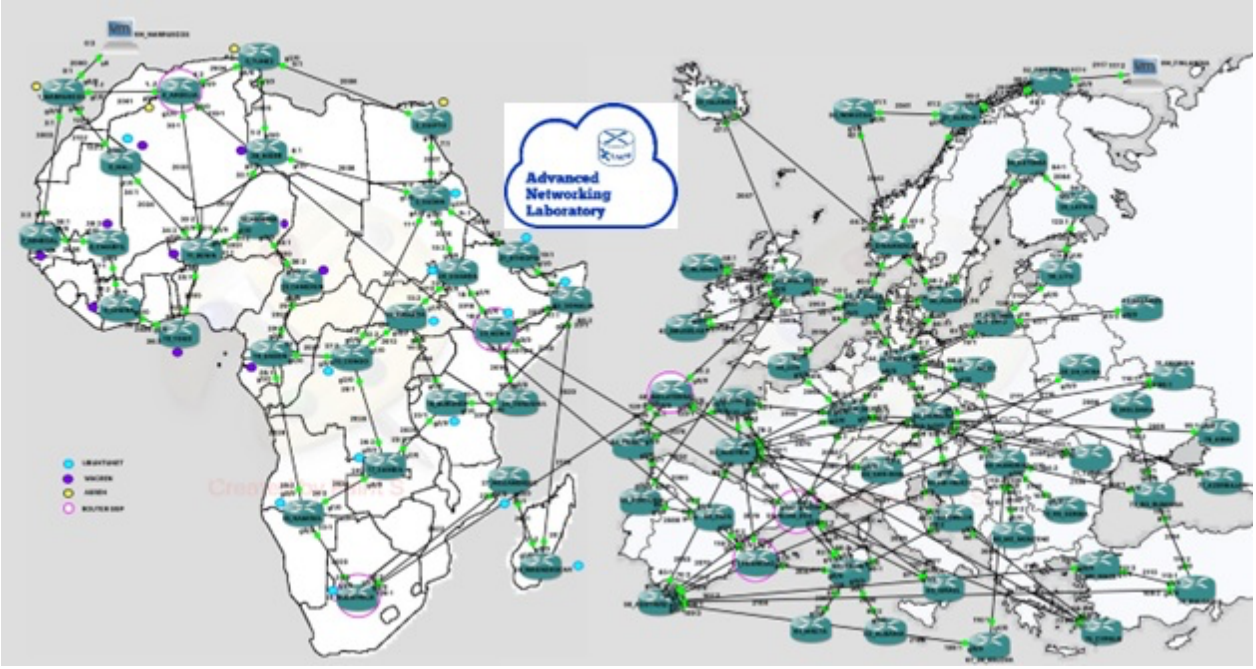


Fig. VIII.13. Emulación de la topología del *backbone* de integrar GEANT y AFRICACONNECT.

Para este caso, la obtención de las tablas de enrutamiento se obtiene mediante la orden “show ipv6 route bgp”.

VIII.10 PRÁCTICA 9: IPv4 vs IPv6

El objetivo de esta práctica es que el lector enlace computadoras bajo IPv4 y bajo IPv6, así como redes exclusivamente bajo IPv6. Utilice simulador y hágalo de manera física.

Actividad 1: Comunique dos computadoras, una bajo una dirección IPv4 y otra bajo una dirección IPv6, para reproducir las topologías indicadas en las figuras VIII.4 y VIII.5

Actividad 2: Reproduzca la red de la figura VIII.8, pruebe la conectividad y realice la gestión completa bajo IPv6.

Actividad 3: Elija una de las topologías de redes avanzadas y comuníquela usando únicamente direcciones IPv6, con sus correspondientes protocolos, para lograr una comunicación completa, así como su gestión completa.

Actividad 4: Realice las pruebas de conectividad IPv6 accediendo a la siguiente dirección: https://test-ipv6.com

Actividad 5: Identifique el grado de adopción de IPv6, así como el nivel de latencia en el país donde vive conectándose a: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

Actividad 6: Revise las páginas web de cada uno de los 5 RIR, con la finalidad de que tenga una idea de qué significan sus siglas y que regiones cubren: ARIN, RIPE NCC, APNIC, LACNIC, AFRINIC.

Actividad 7: Elija dos de las topologías de redes avanzadas y enlácelas usando únicamente direcciones IPv6 y BGP, para realizar la comunicación y gestión completa.

VIII.11 Estado del desarrollo académico global en redes avanzadas

Con la finalidad de revisar el avance que, en el terreno académico, tiene el estudio de las redes avanzadas, se realizó una búsqueda en la base de datos de SCOPUS, con las palabras claves: "*advanced* ***and*** *network* ***and*** *backbone"* **[98]**.

La base de datos de SCOPUS arrojó 891 documentos, sin embargo, dado que SCOPUS rastrea artículos en sus títulos, palabras claves y resúmenes, buscando la coincidencia con alguna de esas palabras claves, muchos documentos hacen referencia al área médico-biológica al encontrar la palabra "advanced". De modo que se realizó una depuración de aquellos documentos que en realidad no tenían relación con las redes avanzadas, a partir de las 23 áreas de conocimiento donde quedaron clasificados todos los documentos. Para ello, se revisó cada uno de los títulos y resúmenes de aquellas áreas poco probables, donde pudiesen quedar los documentos relacionados con las redes avanzadas, y fueron eliminados; y es que, en no pocas ocasiones quienes dan de alta los *conference papers*, no proveen la suficiente información, o quienes catalogan, en muchas ocasiones, lo hacen de manera manual en Elsevier SCOPUS.

A) 8 áreas de conocimiento – 405 publicaciones

De las 23 áreas del conocimiento, después de un exhaustivo refinamiento, se encontraron 405 publicaciones relacionadas con "redes avanzadas", en 8 áreas del conocimiento cuya distribución se indica en la figura VIII.14. Las áreas involucradas son: *Computer science, Engineering, mathematics, physics and astronomy, energy, decisión sciences social sciences y chemical engineering, donde las 2 primeras equivalen al 72%.* **Cada gráfico de este apartado fue tomado directamente de la herramienta de análisis de SCOPUS.**

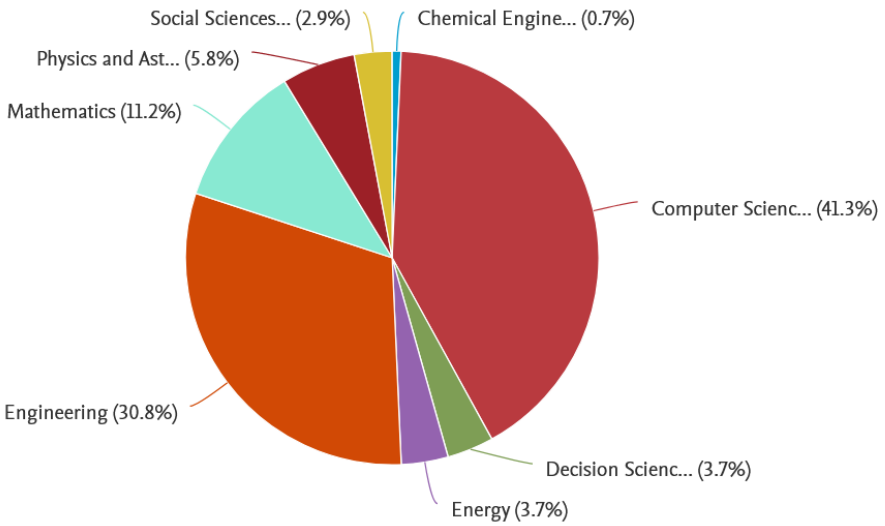


Fig. VIII.14 Publicaciones en "redes avanzadas" en 8 áreas de conocimiento.

El análisis comprende a partir de 1991, cuando apareció la primera publicación respecto de las redes avanzadas, y hasta 2021. A nivel mundial, fue hasta 2017 cuando se superaron las 20 publicaciones anuales en redes avanzadas. La figura VIII.15 indica el número de documentos publicados por año. Cabe señalar que ADVNETLAB, de la UACM, inició aportaciones a publicaciones SCOPUS desde 2016.

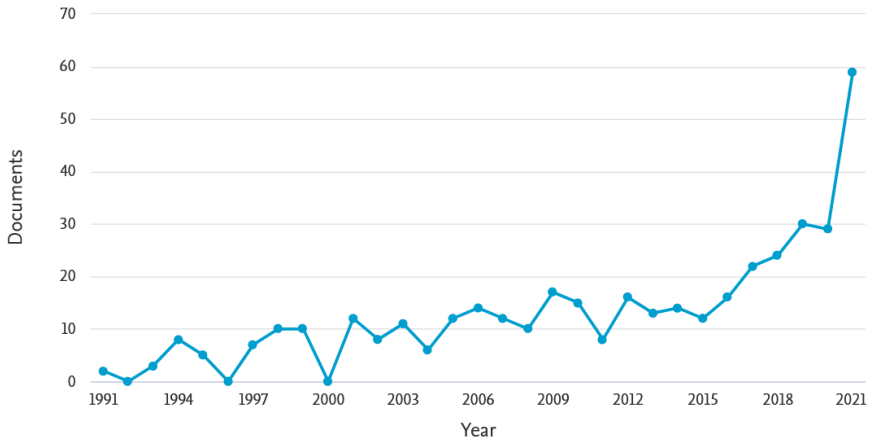


Fig. VIII.15 (405) publicaciones en "redes avanzadas" publicados desde 1991 a 2021.

El 61.5% (249) de las publicaciones son *conference papers*, el 36.3% (147) *articles* y 2.2% (9) son *review papers*. Y, en términos del idioma, la mayoría están en inglés, sólo 17 en chino y 10 en otros 5 idiomas; hay 2 en español. La producción por los 10 países con más publicaciones se muestra en la figura VIII.16, en la que México ocupa el 8vo lugar.

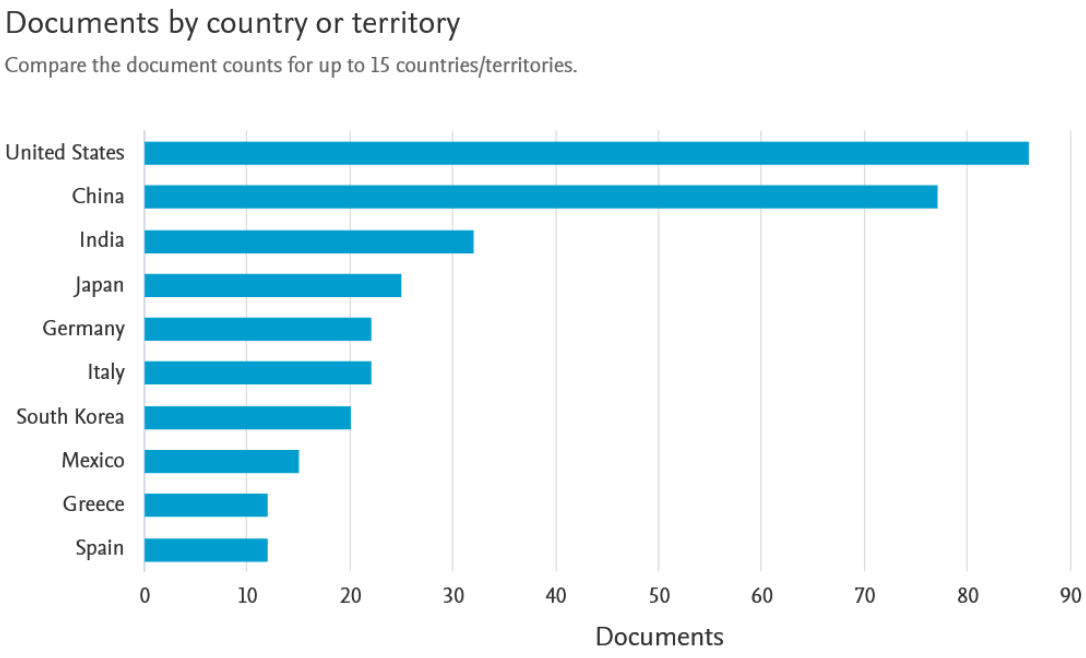


Fig. VIII.16 Número de publicaciones SCOPUS por país, de las 405 publicaciones.

Las 10 instituciones que más producen publicaciones en redes avanzadas se indican en la figura VIII.17, en la que la UACM es la número 1.

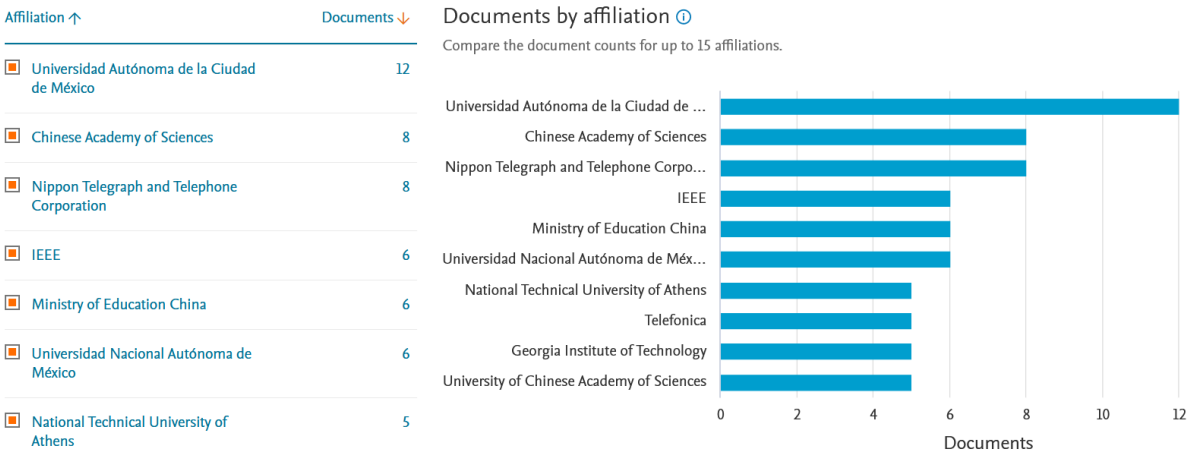


Fig. VIII.17 Publicaciones de las "top 10" instituciones de las 405 publicaciones.

La figura VIII.18 lista a los 10 autores con más publicaciones en "redes avanzadas". Lo que no se indica es la calidad de esas publicaciones.

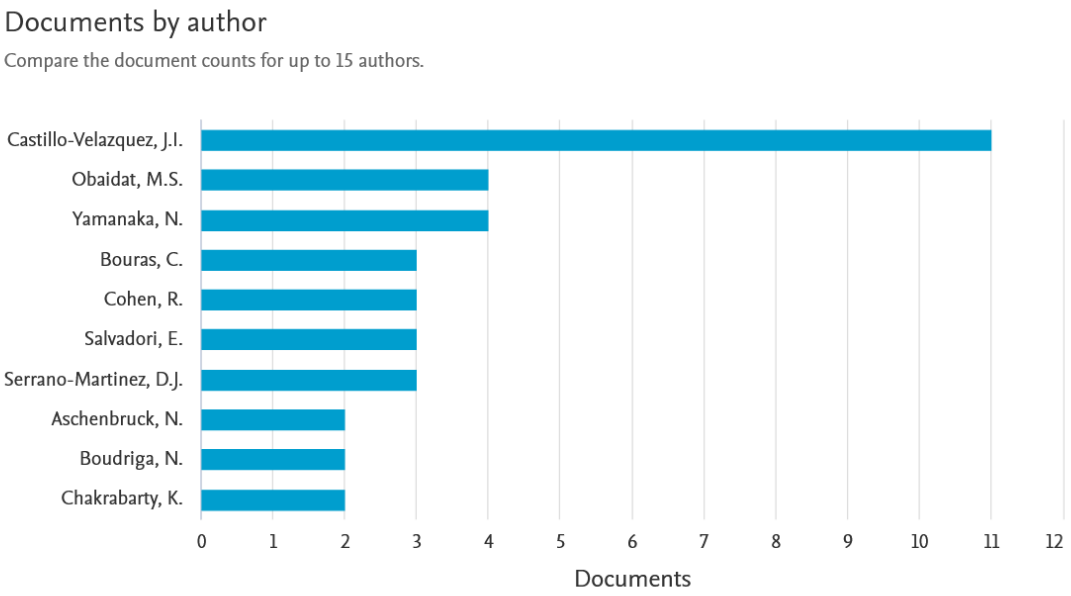


Fig. VIII.18 Los 10 autores con más publicaciones en redes avanzadas.

VIII.12 Huellas digitales de ADVNETLAB-UACM

A continuación, se presentan tanto la huella de colaboración como la huella de presencia en congresos con publicaciones SCOPUS como se indican en las figuras VIII.19 y VIII.20.

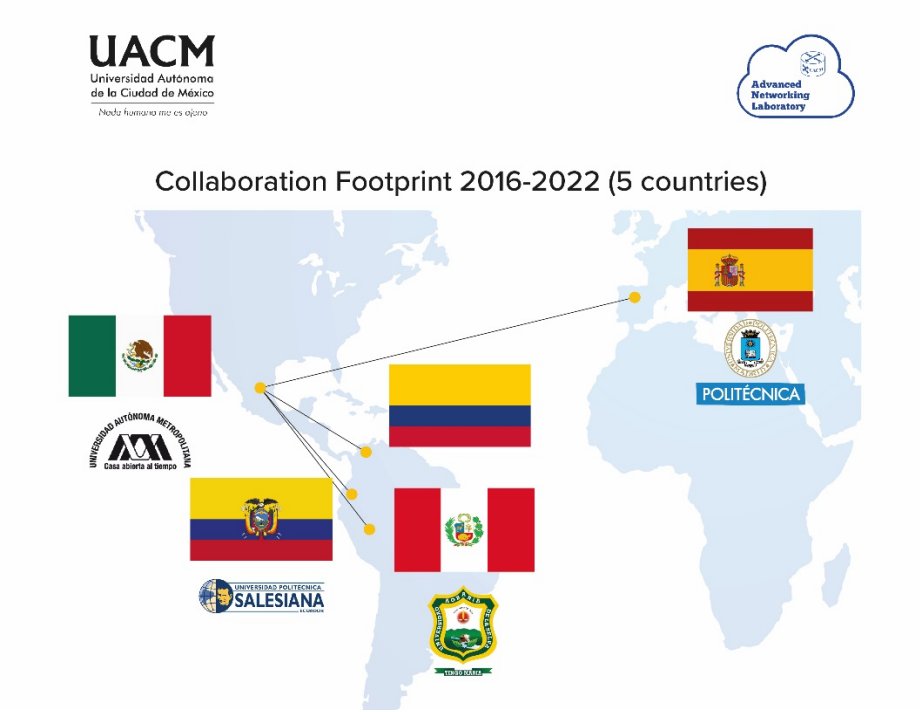


Fig. VIII.19 Huella de colaboración directa e indirecta 2016-2022 (5 países).

Fig. VIII.20 Huella de presencia en congresos con publicaciones SCOPUS 2016-2022 (14 países).

VIII.13 Aportación de la IES Mexicanas a la investigación académica en TICs

Ofrezco el siguiente análisis para intentar responder una de las preguntas más recurrentes de nuestros estudiantes de ingeniería, y en particular del área de las TICS (computación, electrónica y telecomunicaciones), respecto del avance que tiene la UACM con respecto de otras instituciones de educación superior en México.

Contexto respecto de las asimetrías en lo temporal, financiera y de funciones

a) Temporal: En el mundo y en México, hay instituciones que tienen más de 100 años y otras recién creadas en este siglo. Si seguimos una proyección lineal, con recursos y funciones similares, esperaríamos que esas instituciones fueran acumulando producción académica y al final del conteo, la institución más antigua tuviera más producción, pero no siempre es el caso.
b) Recursos: Independientemente del origen de los recursos, públicos o privados, si consideráramos a instituciones con similares funciones y fechas de creación, aquella institución con más recursos económicos puede contratar a más profesores investigadores (considerando que todos tuvieran una calidad y productividad similar), invertir en infraestructura y, así, generar más productos de investigación científica.
c) Funciones: Si consideramos a instituciones de similar temporalidad y recursos (la energía y el músculo para la productividad), las funciones podrían no ser las misas, es decir, algunas instituciones cubren educación media superior además de licenciatura y posgrados como UNAM, IPN, ITESM, BUAP; otras cubren lo mencionado, excepto educación media superior, como UAM y UACM y otras sólo cubren posgrados, como CINVESTAV, COLMEX (aunque tiene una licenciatura) u otros centros de investigación.

Con base en lo anterior, presento: a) Un análisis comparativo respecto de la proporción del volumen de publicaciones y la cantidad de sus autores; b) un análisis comparativo respecto del área de conocimiento de “Engineering” y c) otro respecto del área de conocimiento de “computer sciences”, las dos que cubren las áreas de las TICS.

A. La proporción de publicaciones contra el número de autores

Si contabilizamos los documentos producidos por una institución y el número de autores de la institución que lo producen, podemos medir la "taza de publicaciones SCOPUS *vs* autores", para cada una de las instituciones seleccionadas; el resultado se muestra en la figura VIII.21. ¿Cuántas publicaciones SCOPUS, exclusivamente por afiliación, tiene cada institución? Se indica el año de fundación, como referencia, y a continuación, se revela información interesante. Todos los productos son arbitrados, por estar en SCOPUS, estos incluyen artículos en revistas, artículos en congresos, libros y capítulos de libros. Los autores son los investigadores o profesores investigadores y estudiantes involucrados, activos o egresados.

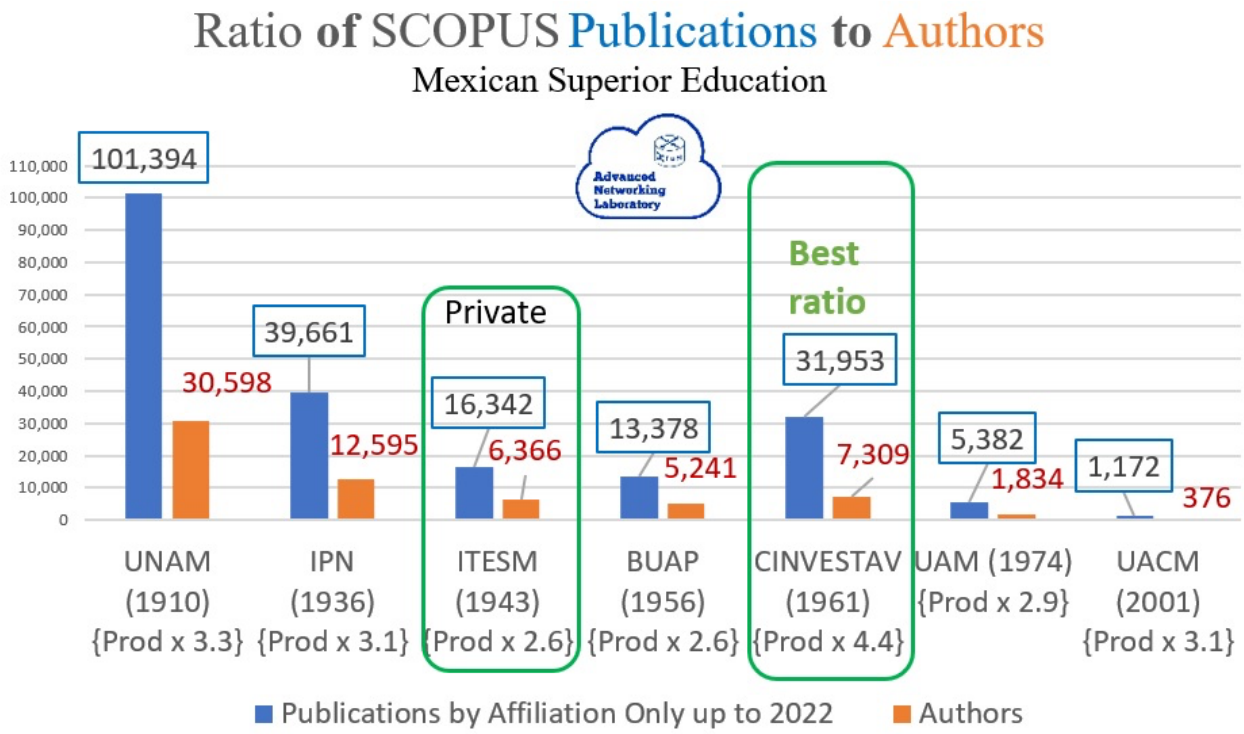


Fig. VIII.21 Razón de publicaciones (solo por afiliación) a autores – Instituciones mexicanas

En la figura se observa que el **Centro de Investigación y Estudios Avanzados del IPN** (CINVESTAV) es la institución con mejor tasa de productividad. Esto es de esperarse, porque sólo atiende a posgrados, con presupuesto amplio y académicos con funciones de "investigador". Y, si bien, el CINVESTAV es el tercer mayor productor de publicaciones, también lo es en mayor número de autores. Un resumen de funciones y productos se indica en la figura VIII.22 **[99].**

CINVESTAV a 2020 (Fundado 1961)

Elaborado por con base en el análisis del ejercicio 2020 del presupuesto de egresos del CINVESTAV del IPN, cuenta pública gobierno de México.

Finalidad	Función	Productos	Presupuesto 2020
1.Gobierno	Coordinación de la política de gobierno	Mejora de controles internos y auditoria	0.2%
2.Desarrollo social	Educación	➢ **2970** alumnos en 66 programas de posgrado (33M/33D). ➢ **596** grados de Maestría y Doctorado	41.5%
3.Desarrollo económico	Desarrollo social	➢ 1,636 artículos publicados (arbitraje estricto) ➢ Mantiene 654 proyectos CYT	58.3%
			$ **2,915**,916,600.00

Fig. VIII.22 Funciones, productos y presupuestos para el CINVESTAV en 2020.

En contraste, en el otro extremo, con otro presupuesto y funciones, tenemos a la Universidad Autónoma de la Ciudad de México (UACM), fundada 40 años después que CINVESTAV, con un presupuesto anual de casi el 50% que aquel, para atender a más de 20,000 alumnos, en 28 programas, 20 de licenciatura, 7 de maestría y 1 doctorado; es decir, una universidad más enfocada en la docencia que en la investigación. Además, el CINVESTAV es una institución dedicada exclusivamente a la ciencia y tecnología, con casi 635 investigadores, mientras que la UACM tiene el 35% (7) de sus licenciaturas, el 37% (3) de sus posgrados y al 33% (325) de su personal en ciencia y tecnología.

Si comparamos la taza de publicaciones a autores, CINVESTAV tiene la más alta de México: con 4.4, contra un 3.1 de la UACM, lo cual resulta revelador para una institución tan joven, pequeña y con recursos limitados como la UACM. En CINVESTAV los investigadores lo son de tiempo completo, es decir, 40 horas, con un apoyo a 654 proyectos que, además, acceden a presupuestos de CONACYT; mientras que en la UACM los profesores investigadores, en el mejor de los casos, tienen 20 horas de investigación, sin un área de investigación formal y con un apoyo simbólico para escasos 12 proyectos en 2022 **[100]**.

Y si bien este análisis fue general y no exhaustivo, veamos ahora cómo están las instituciones en las áreas de nuestro interés donde se ubican las publicaciones de las TICS.

B. Comparación por áreas de conocimiento: *Engineering*

No todas las instituciones tienen un desempeño homogéneo, de modo que las comparaciones deben hacerse entre carreras o entre áreas de conocimiento. Es por ello que, proveeré análisis comparativos para las áreas de conocimiento *Engineering* y *Computer Sciences*, las dos únicas afines a nuestro interés y definidas en la base de datos de SCOPUS con las áreas TICS, dado que es la que emplea globalmente la UNESCO. SCOPUS divide el conocimiento en 26 áreas y sólo las dos indicadas son compatibles con el área de las TICS, aun cuando, por errores de catalogación, algunas de las publicaciones se colocan en alguna de otras áreas, como en *decision sciences, chemical engineering, mathematics* y *physics and astronomy,* por lo que siempre requiere hacer los refinamientos y acotaciones necesarios. Entonces, ¿cómo vamos en la producción académica en ingeniería y cómo se dan estas tendencias? ¿Alguien está invirtiendo correctamente y alguien se está estancando? Me limito a ofrecer los registros internacionales y no abordo las causas. En el gráfico de la figura VIII.23, podemos observar varios fenómenos interesantes: las líneas punteadas coinciden con los sexenios presidenciales mexicanos para calcular el crecimiento cada 6 años.

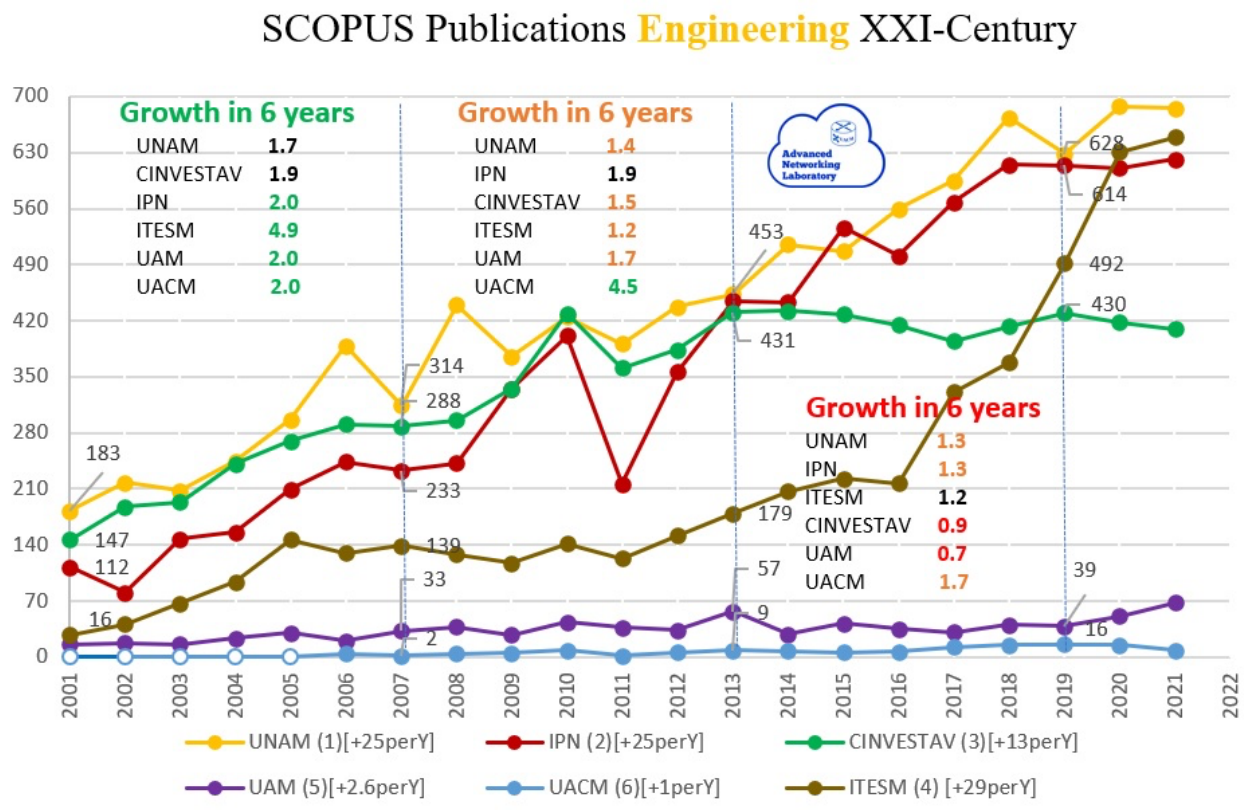


Fig. VIII.23 Productos SCOPUS en ingeniería de 2001 a 2021 para algunas instituciones mexicanas.

En la parte inferior, se indican las posiciones en *rankings,* en términos del número de publicaciones totales donde, por su presupuesto y longevidad, la UNAM lidera, como se esperaba.

Obsérvese que el ITESM, la única institución de educación superior privada analizada, va acelerando con un ritmo exponencial desde 2016 después de un estancamiento de 2005 a 2012; mientras que las instituciones públicas, consideradas líderes, presentan una muy notable desaceleración, donde quizás el caso más dramático es el del CINVESTAV, el cual está estancado en ingeniería, desde el año 2010, de modo que no supera los 431 artículos por año. A este ritmo, el ITESM podría superar, en producción académica en ingeniería a la UNAM, en 2023. Por otro lado, obsérvese que la UACM generó su primer producto en 2006, cuando sólo contaba con 3 carreras de ingeniería en tres campus; mientras que el primer egresado de ingeniería se logró en el año 2012, en la carrera de ingeniería en transporte urbano. En el mismo gráfico, también se calculó el número promedio de artículos que las instituciones incrementan a su producción cada año, por ejemplo, la UNAM y el IPN agregan cada año en promedio 25 artículos a su producción. Es natural esperar un estancamiento, por efectos colaterales de la pandemia a partir del año 2020.

Una reflexión más, el CINVESTAV ha producido un máximo de 432 productos en su año más productivo. Entonces, si tuviese un sexto del presupuesto que tiene y sus investigadores fueran profesores-investigadores, de modo que sólo pudiesen dedicarle el 50% del tiempo que le dedican a la investigación, y si el número de publicaciones impactara linealmente, entonces esta institución tendría aproximadamente 36 publicaciones por año, es decir, el número de publicaciones que debería producir anualmente la UACM, en su año más productivo, si consideramos los factores de presupuesto y tiempo (haciendo una normalización). Claro está que este análisis considera la producción cuantitativamente.

C. Comparación por áreas de conocimiento: *Computer sciences*

En la figura VIII.24, podemos observar varios fenómenos interesantes. Quizás el más relevante es el crecimiento exponencial del ITESM, institución que en 2021 superó en producción anual al líder en periodos previos, el IPN. El *ranking* se indica en la parte inferior del gráfico. Si bien, en el primer sexenio del siglo XXI, se presenta, en lo general, un crecimiento superior a un factor de 2; en el segundo y tercer sexenio en lo general se observa una desaceleración, la cual no es tan dramática, como en el caso de la ingeniería. De manera similar al caso de ingeniería, en computación, el CINVESTAV presenta la más fuerte desaceleración, que de 2010 a 2021 lo deja con un promedio de casi 275 productos anuales y, a ese ritmo, perderá la tercera posición general en 5 años. Mientas, ya es el cuarto lugar desde 2019 en producción anual (a 100 publicaciones anuales de la UNAM, la cual ocupa el tercer lugar).

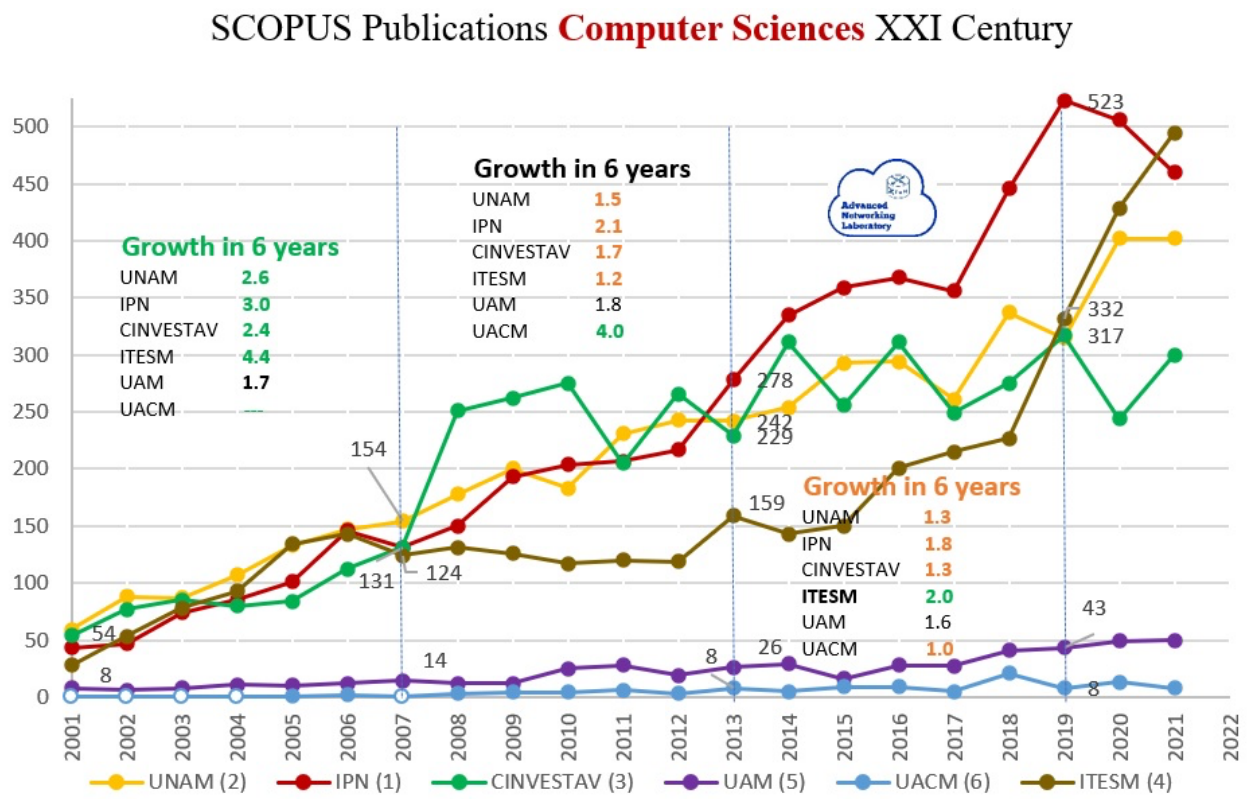


Fig. VIII.24 Productos SCOPUS en computación de 2001 a 2021 para instituciones mexicanas.

En caso de que el ITESM mantenga su ritmo de crecimiento, este sexenio se acerca al factor 4, y si las instituciones públicas continúan su estancamiento, en 2025, superará al CINVESTAV en el volumen general, en computación; en 2028, a la UNAM y en 2030 al IPN. Siempre se trata de qué hacen unos y que dejan de hacer otros, por diversos motivos, como sucedió entre EUA y China.

VIII.14 EVALUACIÓN PARTE IV

Tiempo máximo: 60 minutos. Lea cuidadosamente. El instrumento contiene reactivos del nivel cognitivo "recordar" (conocer), cuyo valor es 1 punto, reactivos del nivel cognitivo "comprender", cuyo valor es 2 puntos; y reactivos del nivel cognitivo "aplicar", cuyo valor es 3 puntos.

Parte I (10 pts.)

1. Indique cómo se obtiene el número máximo de direcciones disponibles para IPv4 y para IPv6 (2 pts.).

2. Use un simulador para conectar dos computadoras, empleando direcciones IPv6 y no IPv4. Para ello active ARP e ICMP, de modo que pueda visualizar la prueba de conectividad vía ping (2 pts.).

3. Tunelamiento entre IPv4 e IPv6: Realice una simulación a modo de comunicar dos computadoras donde una tenga su NIC configurada con IPv4 y la otra con su NIC con figurada en IPv6. Pruebe la conectividad en ambas direcciones (3 pts.).

4. Use un emulador para probar la conectividad y gestión de la topología de la figura VIII.12 bajo IPv6 (3 pts.).

Apéndice A: Sistemas de comparación académica y transferencia de riqueza.

Desde que se crearon las métricas de volumen de producción, nacieron las críticas en el mismo ambiente académico y, de manera global desde la década de los 50. Hoy, incluso la revista Nature, creó su propio *Nature Index* y que concuerda con las recomendaciones de *San Francisco Declaration on Research Assesssment* (DORA), emitido en diciembre de 2012, en San Francisco California, EUA. Esta declaración es breve y recomiendo su lectura. Uno de sus postulados es el siguiente **[101]**:

> "Cuando se compara la calidad de la investigación y el desempeño institucional se deben considerar múltiples factores, ya que los resultados de la investigación científica no sólo incluyen artículos de revistas, sino también datos, software, propiedad intelectual y científicos jóvenes altamente capacitados". …….El factor de impacto de las revistas puede ser manipulado (o truqueado) por la política editorial ……

A) Argumento contra la comparación genérica vacía (zanahorias *vs* manzanas)

Declaraciones como las de DORA surgen de viejas inquietudes. Desde 1996, ya había críticas manifestadas globalmente acerca de la inexactitud e imprecisión de los sistemas de medición y los rankings generales. Y es que las comparaciones muy generalizadas quedan vacías y no sirven, ni a inversionistas, ni a tomadores de decisiones. Por ejemplo, cuando se comparan dos instituciones de educación superior, una de ellas ofrece 100 carreras y la otra ofrece 10 carreras. Ahora bien, suponiendo, en el mejor de los casos, que las 10 carreras de la segunda institución concuerden exactamente con 10 carreras de las 100 de la primera de éstas, aun así es como comparar zanahorias con manzanas. Hay cientos de ejemplos por tratar, pero no es el objetivo en esta obra, sólo nos basta con dejar claro que la propaganda empujada por los grandes intereses globales de las empresas de *rankings* no es para nosotros; pues debemos interesarnos en las comparaciones por áreas de conocimiento o, de modo más puntual, por carreras.

B) La transferencia de riqueza

En 1955, el lingüista Eugene Garfield de EUA, fundó el *Institute for Scientific Information* (ISI) para generar un listado bajo un índice de "las mejores" publicaciones académicas en todos los campos del conocimiento. El índice se conoce como *Science Citation Index* (SCI) y consiste en medir el número de citas de las revistas a través de la suma de las citas de cada artículo. Con el tiempo se generaron otras métricas, incluso se creó la bibliometría y el análisis bibliométrico, con

la finalidad de medir, cuantitativa y cualitativamente, la producción académica. En 30 años, el SCI se hizo muy popular, pero para 1982 fue difícil para ISI mantener el creciente volumen de publicaciones y las críticas ya eran amplias y contundentes, pese a ello, el ISI pudo venderse a la poderosa Reuters, por más de 210 MDD **[102]**. Este hecho no es trivial, ya que incitó a otros a crear instituciones con fines de lucro (algunas instituciones dicen que no lo son, pero obtienen millones de dólares anualmente) para realizar mediciones y comparaciones académicas con una infinidad de métricas. El *boom* llegó en la década de los 90. Las críticas a este modo de transferencia de riqueza ya eran tales al principio del siglo XXI, que, para 2012, en el mismo país que se creó el ISI, paradójicamente también se creó la citada declaración DORA. En 2005 se publicó el "índice h", como métrica de la productividad individual de los investigadores en función del número de citas que reciben sus productos, la cual tuvo una gran aceptación; y, pese a las críticas acerca de las limitaciones de esa métrica, hoy es la más usada globalmente en términos bibliométricos.

La transferencia de riqueza opera cuando las editoriales cobran cantidades que van desde los 10 hasta los 100 dólares, para que un usuario acceda a un artículo, si una revista no es *open Access;* o en las revistas *Open Access,* pueden cobrarle al autor entre 2,000 a 5,000 dólares. Ese dinero, no beneficia a los autores sino a las editoriales, y dado que la mayoría de las editoriales son de los EUA y europeas, la transferencia de riqueza se da desde quienes financian las publicaciones del resto de los continentes hacia las editoriales cuya lengua materna preferentemente es el inglés. Sin embargo, desde 2010, los países del continente asiático están equilibrando la balanza poco a poco.

Apéndice B: Principales acrónimos

ATM - *Asynchronous Transfer Mode*

AS – *Autonomous System*

ASBR - *Autonomous System Backbone Router*

BGP - *Border Gateway Protocol*

CAHU – *Central Air-Handling Unit*

CCCU – *Close Coupled Cooling Unit*

CLARA – Cooperación Latinoamericana de Redes Avanzadas

CRAC – *Computer Room Air Conditioning*

CRAH - *Computer Room Air Handler*

CUDI – Consorcio Universitario para el Desarrollo de Internet

CUE – *Carbon Usage Effectiveness*

DCE – *Data Center Effectiveness*

GEANT – Gigabit European Advanced Network

ICREA – *International Computer Room Experts Association*

IDF - *Intermediate Distribution Facility*

ISDN – *Integrated Services Digital Network*

ISP - *Internet Service Provider*

MAN – *Metropolitan Area Network*

MDF - *Main Distribution Facility*

MIB – *Management Information Base*

MRSFA – *Modem, Router, Switch, Firewall y Access point*

NIC & WNIC – *Network Interface Card y Wireless NIC*

NMS - *Network Management System*

ONT – *Optical Network Terminal*

OSPF – *Open Shortest Path First*

PUE - *Power Usage Effectiveness*

PSTN - *Public Switching Telephonic Network*

RIP – *Routing Information Protocol*

SAN - *Storage Area Network*

SNMP – *Simple Network Management Protocol*

SPD – *Surge Protective Device*

UPS - *Uninterruptible Power System*

WAN - *Wide Area Network*

WUE - *Water Usage Effectiveness*

REFERENCIAS

PARTE I

1. José Ignacio Castillo Velázquez, *Switching & Routing*: Introducción, México, Samsara Editorial, 2016. ISBN: 978-970-94-2977-0.
2. José Ignacio Castillo Velázquez, *Redes de datos: contexto y evolución*, 3ª Ed. México, Samsara Editorial, 2019. ISBN: 978-970-94310-9-4.
3. DEC-INTEL-XEROX, *The Ethernet, a Local Area Network Data Link Layer and Physical Layer Specifications Version 2.0*, USA, Nov. 1982.
4. *ISO 7498:1984 Open Systems Interconnection – Basic Reference Model: The basic Model, 1984.*
5. *ISO 7498-2:1989 Information Processing Systems – Open Systems Interconnection – Basic Reference Model-Part 2: Security Architecture, 1989.*
6. *ISO/IEC 7498-1:1994 Information Technology – Open Systems Interconnection – Basic Reference Model: The basic Model, 1994.*
7. *ISO/IEC 7498-3:1997 Information Technology – Open Systems Interconnection – Basic Reference Model: Naming and Addressing, 1997.*
8. IEEE Std 802.3, IEEE standards for LAN & WAN: Overview and architecture, 2002.
9. Cisco, End-of-Life Announcement of the Cisco FastHub 100, 200 and 300 Series, Product bulletin 891, Ca. USA, 1999.
10. Cisco, End-of-Sale Announcement of the Cisco FastHub 400 Series, Product bulletin 1715, Ca. USA, 2002.
11. Cisco, IP Addressing and Subnetting for new users, Cisco Press, pp. 4-10, 2005.

PARTE II

12. DARPA, RFC 1009, *Requirements for internet gateways*, June 1987.
13. DARPA, RFC 1716, *Towards requirements for IP routers*, Nov 1994.
14. DARPA, RFC 1093, *NSFNET Routing Architecture*, 1989.
15. DARPA, RFC 1812, *Requirements for IP Version 4 Routers, Jun 1995.*
16. Fang Luyuan, Zhang Raymond, Taylor Michael, Evolution of carrier Ethernet Services-Requierements and deployment case studies, IEEE Communications Mag Vol46, No. 3, March 2008, pp. 69-76.
17. Samer Salam and Ali Sajassi, provider backbone Bridging and MPLS: complementary technologies for next-Generation carrier Ethernet transport, IEEE Communications Mag. Vol. 46, No. 3, March 2008, pp. 77-83.
18. DARPA, RFC 1058, *Routing Information Protocol*, Jun, 1988.
19. DARPA, RFC 1388, *Routing Information Protocol V2*, Jan, 1993.
20. Internet Standard, RFC 1723, *Routing Information Protocol V2*, Nov, 1994.
21. Internet Society, RFC 2453, *Routing Information Protocol V2*, Nov, 1998.
22. IETF, RFC 4822, *RIP V2*, Feb, 2007.
23. Hedrick, C., RFC 2080, *RIPng for IPv6*, Jan, 1997.
24. IEFT, RFC 1131, The OSPF specification, Oct 1989.
25. IEFT, RFC 1247, OSPF Version 2, July 1991.

26. IEFT, RFC 1248, OSPF Version 2 Management Information Base, July 1991.
27. IEFT, RFC 1583, OSPF Version 2, March 1994.
28. IEFT, RFC 2178, OSPF Version 2, July 1997.
29. IEFT, RFC 2328, OSPF Version 2, Apr 1998.
30. IEFT, RFC 2740, OSPF for IPv6, Dec 1999.
31. IEFT, RFC 5340, OSPF Version 3, July 2008.

PARTE III

32. Castillo José Ignacio, Et al., SCRTI-UACM, Documento de dictamen técnico SCTRTI-CAAPS/UACM/2010/02, 23 de marzo de 2010.
33. Castillo-Velázquez José-Ignacio, Galicia-Gutiérrez Noe, López-Ruiz Juan-Arnulfo, *Ingeniería inversa parcial y simulación de la infraestructura de una red de datos MAN*, ROC&C, México, 2013.
34. UPTIME Institute, https://es.uptimeinstitute.com
35. ICREA, Standard ICREA 131-2021 http://www.icrea-international.org
36. The Green Grid, Whitepaper #32, Carbon Usage Effectiveness (CUE): A Green Data Center Sustainability Metric, 2010.
37. The Green Grid, Whitepaper #35, Water Usage Effectiveness (WUE): A Green Grid Data Center Sustainability Metric, 2011.
38. TIA-942 Data Center Standards Overview, White Paper, 2005.
39. The Green Grid, Whitepaper #36, Data Center Maturity Model, 2011.
40. UNCTAD, Technology and Innovation Report 2021: catching technological waves innovation with equity, pp.110-140, Geneva, 2021.
41. Case, J., Fedor M., Davin J., IEFT, RFC 1067, A Simple Network Management Protocol, August 1988.
42. Case, J., Fedor M., Schoffstall M., Davin J., IEFT, RFC 1098, A Simple Network Management Protocol (SNMP), April 1989.
43. Case, J., Fedor M., Schoffstall M., Davin J., IEFT, RFC 1157, A Simple Network Management Protocol (SNMP), May 1990.
44. Case, J., McCloghrie K., Rose M., Walsbusser S., IEFT, RFC 1448, Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), April 1993.
45. Case, J., McCloghrie K., Rose M., Walsbusser S., IEFT, RFC 1905, Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), January 1996.
46. Presuhn R., Case, J., McCloghrie K., Rose M., Walsbusser S., IEFT, RFC 3416, Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), Internet Standard, December 2002.
47. Rose M., IEFT, RFC 1215, a convention for defining Traps for use with the SNMPv2, March 1991.

PARTE IV

48. IBM SPSS Statistics *Data sheet*, [Disponible en https://www.ibm.com/products/spss-statistics/support, última visita octubre de 2022]
49. GNS3, 2022 www.gns3.com
50. J. I. Castillo and N. Galicia, "Routing algorithms applied to an advanced academic network know as CUDI," *IEEE Latin America Transactions*, vol. 14, no. 6, pp. 2974-2979, June 2016.
51. José Ignacio Castillo Velázquez, Dictamen técnico para el ingreso de UPAEP a I2 vía CUDI, diciembre, 2003.
52. Adam Stone, *Internet2's Breakthroughs for Academic Research*, IEEE Distributed Systems Online, Computer, Vol. 5, N1, January 2004. ISSN:1541-4922.
53. U. Chomicka, *Internet2's Global Programs: International Connectivity*, Internet2, JET Meeting, February 2016.
54. School of medicine & Health Science, *institutions Connect to the Nation´s Fastest Research & Education Network to Benefit Health Researchers Nationwide*; February 26, 2014.
55. J. -I. Castillo-Velazquez, D. -J. Serrano-Martinez and A. Morales, "Emulation of the connectivity of backbone and management for the layer 3 service of INTERNET2: 2016 topology," 2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII), 2017, pp. 1-4, doi: 10.1109/CONCAPAN.2017.8278476.
56. CANARIE, *Revolutionary human brain atlas created by Canadian-German team one of top 10 breakthrough technologies of 2014*.
57. Leslie Regan S., *Computer Networking in Canada: from CA*net to CANARIE,* Canadian Journal of Communication, Vol 19, N1, 1994.
58. J. -I. Castillo-Velazquez and A. Delgado-Villegas, "GNS3 Limitations when Emulating Connectivity and Management for Backbone Networks: A Case Study of CANARIE," *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, London, ON, Canada, 2020, pp. 1-4
59. Red CLARA http://www.redclara.net/ [Última visita: febrero de 2022]
60. J. Castillo-Velazquez and J. Sánchez-Trejo, "Emulation for CLARA's operation, the advanced network for Latin America," *2016 IEEE ANDESCON*, Arequipa, 2016, pp. 1-4.
61. J. Castillo-Velazquez, D. Serrano-Martinez and A. Morales, "Emulation of backbone's connectivity and management for the advanced network in Latin America: 2016's topology," *2017 Sensors Networks Smart and Emerging Technologies (SENSET)*, Beirut, 2017, pp. 1-4.
62. CUDI 2, http://www.cudi.edu.mx/ [Última visita: febrero de 2022]
63. Dyer J. Haver M and Nowlan M, *ASPIRE: a study on the prospects of the Internet for research and education 2014-2020*, TERENA, 2014. ISBN: 978-90-77559-22-2.
64. GEANT Anual report 2018, Collaboration Projects, 2018.
65. GÉANT, *GÉANT and outGRID – Underpinning a global neuroscience grid infrastructure: case study 2017., EU.*
66. J. -I. Castillo-Velazquez, I. Muñoz-Martínez, J. -A. Díaz-Ramírez and E. F. Ordoñez-Morales, "Management Emulation for GEANT Advanced Network: 2020 Topology under IPv6," 2020 IEEE ANDESCON, 2020, pp. 1-6, doi: 10.1109/ANDESCON50619.2020.9271972.
67. AFRICACONECT, Node site, 2020 www.africaconnect2.net
68. J. -I. Castillo-Velazquez and L. -C. Revilla-Melo, "Management Emulation of Advanced Network Backbones in Africa: 2019 Topology," 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),

London, ON, Canada, 2020, pp. 1-4.

69. APAN, Proceedings of the 48th meeting of the Asia Pacific Advanced Network, 2019.
70. PACIFIC WAVE, Node Site, 2020 www.pacificwave.net.
71. DARPA , RFC 1105, *Border Gateway Protocol BGP*, 1989.
72. Lougheed, K., and Y. Rekhter, RFC 1267, "A Border Gateway Protocol 3 (BGP-3)", Cisco Systems, T.J. Watson Research Center, IBM, Corp., October 1991.
73. Rekhter, Y., and T. Li, RFC 1654, "A Border Gateway Protocol 4 (BGP-4), July 1994.
74. Y. Rekhter, T Li, S Hares, RFC 4271, A Border Gateway Protocol-4, July 2006.
75. Marques P., Dupont F., RFC 2545, "Use of BGP-4 multiprotocol Extensions for IPv6 Inter domain Routing", March 1999.
76. C. -V. Jose-Ignacio, D. -J. Serrano-Martinez and H. Mónica, "Management Emulation for Advanced Networks Interconnection in all America: 2019 topology," 2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX), 2019, pp. 1-6, doi: 10.1109/CONCAPANXXXIX47272.2019.8976946.
77. S. Deering, Xerox PARC, R. Hinden, Ipsilon Networks. "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, December 1995
78. S. Deering, Cisco, R. Hinden, Nokia. "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
79. Leavitt N, IPv6: Any closer to adoption? IEEE Computer, 2011.
80. Test connectivity for IPV6, 2022, [Disponible en: https://test-ipv6.com]
81. Google, IPv6 Adoption, 2022, https://www.google.com/intl/en/ipv6/statistics.html
82. R. Coltun, D. Ferguson, J. Moy, OSPF for IPv6, RFC 2740, December 1999.
83. R. Coltun, D. Ferguson, J. Moy, A. Lindem, OSPF for IPv6, RFC 5340, July 2009.
84. Levi, D., Meyer P., Stewart B., IEFT, RFC 2263, SNMPv3 Applications, January 1998.
85. Levi, D., Meyer P., Stewart B., IEFT, RFC 2273, SNMPv3 Applications, January 1998.
86. Case J., Mundy R., Partain D., Stewart B., IEFT, RFC 2570, *Introduction to Version 3 of the Internet-Standard Network Management Framework,* April 1999.
87. Case J., Mundy R., Partain D., Stewart B., IEFT, RFC 3410, *Introduction and Applicability Statements for Internet standard management Framework (SNMPv3)*, December 2002.
88. Schoenwaelder J., Single Network Management Protocol (SNMPv3) Context Engine ID Discovery, RFC 5343, September 2008.
89. Gilmore J., "Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design", Ed. O'Reilly, USA, 1998.
90. FIPS, Advanced Encryption Standard, Federal Information Processing Standards 197, USA, 2001.
91. Rogaway P. (2011) Evaluation of some block cipher modes of operation, UC David USA.
92. BitTorrent, 2022, https://www.bittorrent.com/
93. Rivest R., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of ACM, Vol 21(2), pp120-126, 1978.
94. Rivest R., The MD5 Message-Digest Algorithm, RFC 1321, 1992.
95. NIST, Maintenance Testing for the Data Encryption Standard: Special publication. National Institute of Standards

and Technology USA, 1980.

96. Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4, Domains without Explicit Tunnels", RFC 2529, 1999.
97. SCOPUS, 2022, www.scopus.com
98. J. -I. Castillo-Velazquez, I. -I. Rosas-Suarez and D. -L. Fernandez-Tinoco, "Management of the Continental Advanced Networks GEANT and AFRICACONNECT Joint as Two Autonomous Systems by BGP-4 Under IPv6: Using Limited Resources," 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM), 2021, pp. 1-6, doi: 10.1109/ETCM53643.2021.9590779.
99. SHCP, Análisis del ejercicio 2020 del presupuesto de egresos del CINVESTAV del IPN, gobierno de México, 2021.
100. UACM, Presupuesto UACM ejercicio 2021, https://uacm.edu.mx/portals/0/tesoreria/Proyecto_Presupuesto_2021.pdf
101. San Francisco Declaration on Research Assessment (DORA), dec. 2012.
102. Rosselli, Diego. (2019). Yo te cito tú me citas: la importancia de las referencias. Acta Neurológica Colombiana. 35. 10.22379/24224022225.

Esta obra se terminó de imprimir en el mes de enero de 2023
en los talleres de Litográfica Ingramex, S.A. de C.V.
Centeno 162-1. Col. Granjas Esmeralda, Iztapalapa
C.P. 09810. Ciudad de México. México.