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

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS
Y DE TELECOMUNICACIONES

"Emulación del Backbone de la red avanzada I2 en México"

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

PRESENTA:

Noé Galicia Gutiérrez

Director del trabajo recepcional

Mtro. José Ignacio Castillo Velázquez

México, D.F. Marzo, 2015.

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

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

AGRADECIMIENTOS

Quiero agradecer especialmente a mis padres por el apoyo y comprensión que me brindaron durante estos años de estudio. Gracias por su paciencia.

Debo agradecer de manera especial al profesor M. en C. José Ignacio Castillo Velázquez por su generosa ayuda en el planteamiento, dirección y revisión de esta tesis.

Así como a cada uno de los lectores que revisaron este trabajo de tesis.

Agradezco a la Universidad Autónoma de la Ciudad de México por el apoyo recibido para la impresión y empastado de este trabajo recepcional.

A todos y cada uno de ustedes……..gracias.

Resumen

Oficialmente la Internet comercial nació en 1995 y se concibe como una gran colección de sistemas Autónomos (AS) para el intercambio de información entre AS.

Internet 2 nació en 1996 en los EE.UU., después en todo el mundo se diseño y se implemento una internet para las universidades y centros de investigación, todas estas nuevas redes de internet 2 son llamadas “redes avanzadas”.

En el caso de México se crea CUDI (Corporación Universitaria para el desarrollo de Internet 2), fundada en 1999 para la implementación de Internet 2 en el país. Internet 2 también se forma como la Internet comercial, porque está integrado por AS, por lo que cada red avanzada cuenta con un número de identificación y el número de identificación para el AS de CUDI es 18592.

A través del tiempo, la red CUDI ha sufrido algunos cambios en su topología, tantos como nuevas redes de afiliados se han integrado y como la red de CUDI ha sido conectada a otras redes avanzadas internacionales en EE.UU. y América Latina, como internet 2 y CLARA.

En 2013 CUDI tenía 266 instituciones como miembros, mientras que para el 2014 contaba con 280 instituciones miembro, con velocidades de 34 Mbps para los miembros asociados, de 2 Mbps para los miembros afiliados, mientras que el Backbone de CUDI con una velocidad de STM-1 (155 Mbps).

Las redes avanzadas permiten aplicaciones en diversas áreas de la ciencia y tecnología como son, las ciencias exactas, medicina o salud, bibliotecas, laboratorios, y verificar nuevos protocolos que serán utilizados en un futuro en las redes de datos.

En el presente trabajo se realizó la emulación del Backbone de la red CUDI, por medio del emulador GNS3, para lo cual se requirió conocer la infraestructura de la red CUDI y posteriormente se verificaron las capacidades del emulador al soportar una red de este tipo, esto se realizo enviando ping entre los quipos que componen esta red.

ÍNDICE

	Pag.
CAPÍTULO 1 Introducción: "Redes Avanzadas"	**1**
1.1 Objetivo	**1**
1.2 Justificación	**1**
1.3 Internet	**2**
1.4 Internet II (I2)	**5**
1.4.1 Arquitectura I2	**7**
1.5 Otras Redes Avanzadas	**9**
1.6 Internet 2 en México	**12**
1.6.1 Infraestructura CUDI	**13**
1.6.2 NOC CUDI	**17**
CAPÍTULO 2 Protocolos de enrutamiento	**18**
2.1 Algoritmos de enrutamiento	**18**
2.2 Protocolos de enrutamiento	**19**
2.2.1 IGP:RIP	**22**
2.2.2 IGP: RIP v2	**25**
2.2.3 IGP: IGRP	**26**
2.2.4 IGP: EIGRP	**27**
2.2.5 IGP: OSPF	**28**
2.2.6 IGP: IS-IS	**35**
CAPÍTULO 3 Simulación del Backbone de la red avanzada I2 en México	**40**
3.1 Introducción	**40**
3.2 Simulación Packet Tracer v5.3	**40**
3.3 Configuración de router y host	**44**
3.4 Simulación	**45**
CAPÍTULO 4 Emulación del Backbone de la red avanzada I2 en México	**63**
4.1 Introducción: Emulación GNS3	**63**
4.2 Configuración de Router	**64**
4.3 Configuración de Host	**65**
4.4 Monitoreo	**70**
4.5 Caracterización del rendimiento del sistema de emulación	**76**
CAPÍTULO 5 CONCLUSIONES	**78**
APÉNDICE A Instalación de GNS3	**81**
A.1 Introducción	**81**
A.2 Instalación de GNS3	**82**

Pag.

APÉNDICE B Direcciones IP **91**
B.1 Introducción **91**
B.2 Direcciones IP **91**
B.3 Subneteo **93**

APÉNDICE C Equipo de Backbone **99**
C.1 Router Cisco 7200 y 7206 **99**
C.2 Router Cisco 7513 **100**
C.3 Router Cisco 7606 **101**
C.4 Router GSR (Gigabit Switch Router) 10000 **102**

APÉNDICE D Comandos de configuración **103**

APÉNDICE E Velocidades de Transmisión **106**

Referencias **108**

Capítulo 1

Introducción: "*Redes Avanzadas*"

En el presente capítulo se presenta una breve reseña del comienzo de ARPANET en los Estados Unidos, la cual dio como resultado en los siguientes años el surgimiento de Internet, para lo cual también se desarrollaron los protocolos TCP/IP. También se aborda el nacimiento de una nueva red llamada Internet 2 o I2 como red de alta velocidad, se describe su topología y arquitectura, en seguida se presentan otras redes avanzadas que se han creado alrededor del mundo, posteriormente se describe el desarrollo de internet 2 en México, su topología e infraestructura.

1.1 Objetivo

1. Realizar una primera aproximación de la infraestructura de la red CUDI mediante un simulador. Forzar al simulador más allá de su uso convencional.

2. Emular la infraestructura de la red CUDI como una segunda aproximación, así como probar las capacidades del emulador.

3. Conocer ha detalle cómo está constituida la infraestructura de telecomunicaciones de la red CUDI.

1.2 Justificación

La finalidad de este trabajo es dar a conocer cómo está constituida la infraestructura de la red avanzada de Internet 2 en México, así como comprobar qué tan viable es simular esta red por medio del simulador Packet Tracer de Cisco, esto porque en cursos de licenciatura difícilmente se pone a prueba la máxima capacidad de los simuladores. Por último se emulará la red de internet 2 de México con la cual se tendrá una mejor aproximación a la red física con la que cuenta y se verificarán las capacidades del emulador GNS3 al soportar este tipo de red.

1.3 Internet

Internet nació en la década de los 60 en Estados Unidos (USA), Paul Baran uno de los arquitectos de la internet construyó en 1964 la primera red de comunicaciones distribuidas, para lo cual dividió la información en bloques de 1024 bits y agregó un encabezado, el mensaje era reconstruido al llegar a su destino. Casi simultáneamente en el Reino Unido Donald Watts Davies implementó un sistema similar al de Baran, le llamó paquetes a los pedazos de información, más tarde estas dos ideas se incorporaron en ARPANET (Advanced Research Projects Agency Network, Red de la Agencia de Proyectos de Investigación Avanzada de los Estados Unidos). [1]

De (1966-1970) ARPA inició un proyecto para conectar a las universidades de Estados Unidos, para ese año ARPA usaba conmutación de paquetes. En 1969 ARPANET o DARPANET creó el protocolo TCP (Transmission Control Protocol, Protocolo de Control de Transmisión) para poder transportar datos entre mainframes.

El 12 de Julio de 1972 Robert Kahn, quien trabajaba en BBN corporation (Bolt, Beranek and Newman), publicó el RFC (Request for Comments) 371 titulado Demonstration at International Computer Communications Conference, indicando que para octubre se pondría a prueba la capacidad de ARPANET para lo cual se daba acceso gratuito a todos los asistentes durante el congreso. Esto requirió conectar el hotel Hilton de Washington a ARPANET. En octubre de ese año se realizó la primera ICCC (International Conference on Computer Communications), evento IEEE, la cual sólo se usaba para compartir recursos mediante accesos remotos a archivos y correos electrónicos una de las herramientas más populares. [2]

Para ese tiempo los primeros nodos de conmutación de paquetes utilizados para conectar las redes hacia ARPANET eran IMP (Interface Message Processor) es decir, la primera generación de Gateway los cuales eran minicomputadoras DDP516 de Honeywell. Los primeros IMP se desarrollaron para UCLA (University of California Los Angeles), SRI (Standford Research Institute), UCSB (University of California Santa Barbara), U.UTAH (University of Utah). El primer enlace se dio entre UCLA y SRI que se conectaban con un enlace físico el cual contaba con 32 enlaces lógicos full dúplex,

el IMP dividía en paquetes de 1010 bits de longitud, que constituían la unidad de transmisión de datos desde un IMP a otro IMP. [3]

En 1973 en Stanford, Vinton Cerf organizó el seminario para el diseño de protocolo huésped “TCP”, para 1975 se liberó la primera versión de TCP, dos años después en 1977 se probó TCP con enlaces satelitales, en ese mismo año ARPANET ve factible tener conexiones de red mediante enlaces satelitales, teléfono y redes de radio para enviar datos a través de ellas. Ese mismo año ARPANET interconectaba 138 mainframes principalmente DEC e IBM, como se muestra en la fig. 1.1. [4]

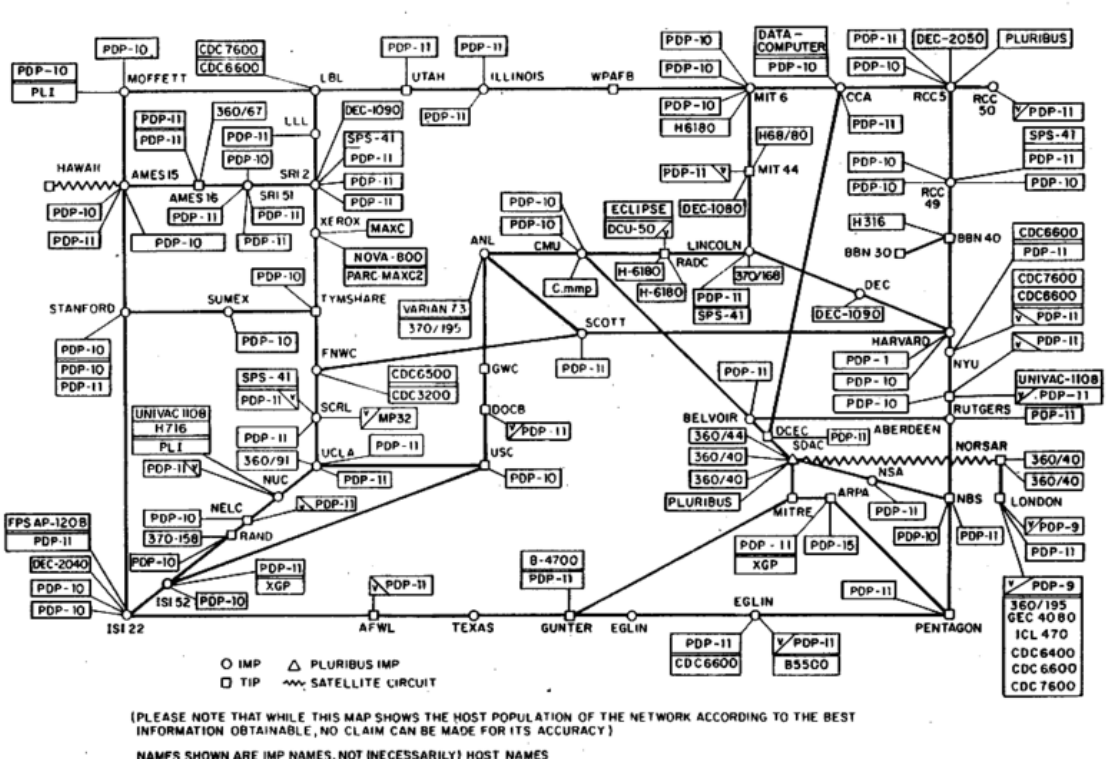

Fig. 1.1 Topología lógica de ARPANET. ARPANET LOGICAL MAP, MARCH 1977 [5]

En 1978 el protocolo TCP se dividió en dos protocolos, un Protocolo de Control de Transmisión (TCP-Transmission Control Protocol) el cual se encarga de ordenar los paquetes, así como la conexión entre los host y un Protocolo de Interconexión (IP-Interconnection Protocol) encargado de enviar paquetes desde servidores y end system a switches o entre ellos. Una vez redefinido TCP/IP por ARPANET, en 1981 se remplazó el Network Control Program (NCP) por TCP/IP y en junio de 1983 TCP/IP

se ejecutaba en todos los host de ARPANET con una velocidad de 45 a 90 Mbps usando fibra óptica, este mismo año se separó la red militar de la red académica por lo que en 1983 se creó la MILNET para comercializar una red civil con el protocolo TCP/IP. Para 1984 ARPANET conectaba a 100 universidades y centros de investigación de Estados Unidos y Europa. Durante esa década proveedores de servicios como CompuServe, America Online y Prodigy daban un servicio comercial en línea por medio del modem a los usuarios de PCs, había nacido la NSFNET (National Science Fundation Network). Un año antes se habían vendido 3.5 millones de PCs, para 1985 2,000 computadoras tenían acceso a internet, para 1987 fueron 30,000 y para 1989 se tenían 160,000 computadoras con acceso a internet.

En 1990 la Universidad de Minnesota introdujo el sistema Gopher el cual ayudaba a los usuarios a tener un mejor manejo y organización de la información, ese mismo año Tim Berners-Lee del CERN (*Conseil Européen pour la Recherche Nucléaire*) desarrolló la World Wide WEB y en diciembre de 1990 ya se tenía la primera versión de la World Wide WEB la cual fue distribuida a otros centros de investigación de física. En 1993 Marc Andreessen quien estaba en NCSA (National Center for Supercomputing Applications) de la Universidad de Ilinois desarrolla un navegador mejorado de la web (Web Browser) llamado Mosaic, el primer sistema que incluía imágenes a color como parte de una página web (web page). Este primer visualizador (browser) estuvo disponible en noviembre del 93, un mes después 40,000 usuarios habían descargado copias de Mosaic y para 1994 1 millón de usuarios, en este mismo año 1994 NCSA desarrolla una versión comercial de Mosaic llamada Netscape, desde ese momento la web y los visualizadores (browsers) también conocidos como navegadores popularizan el internet el cual ha sido el medio más popular para compartir información (video, voz y datos) entre los usuario. En 1995 nace la internet comercial. [1] [6]

Kleinrock, Baran, Davis y Roberts ganaron conjuntamente el “IEEE Internet awards” en el 2000 por sus aportaciones a la tecnología fundacional de la internet. El 6 de junio del 2012 entra en funcionamiento IPv6 el cual está definido en el RFC 2460, este remplazará progresivamente a IPv4 definido en el RFC741. [7]

Actualmente Internet es la sumatoria de todos los Sistemas Autónomos (AS) que se conectan entre sí para transmitir y compartir datos entre AS, como se representa en la ecuación 1.1.

$$Internet = \sum_{i=1}^{n} AS_i \tag{1.1}$$

Representación algebraica de Internet. (M. en C. José Ignacio Castillo Velázquez) [8]

1.4 Internet II (I2).

Internet 2 o I2 es una red de alta velocidad la cual sólo está constituida por universidades y centros de educación o investigación para permitir el intercambio de información e investigación entre estas instituciones, internet 2 está separada de la internet comercial (internet), y no pretende sustituir a internet. En un principio I2 se llamaba UCAID (University Corporation for Advanced Internet Development, Corporación Universitaria para el Desarrollo de Internet Avanzado) la cual estaba integrada por 34 universidades de Estados Unidos en 1996, un año después UCAID cambia su nombre a Internet 2. En 1998 se crea la primera red de Internet 2, la cual fue llamada Abilene, un año después se creó la vBNS (Very High Speed Backbone Network Service, Servicio de Red Backbone de muy alta velocidad) desarrollada por NSF (National Science Foundation's, Fundacion Nacional de la Ciencia), fig. 1.2.

Para el 2003 el backbone de Abilene (Internet 2) era una red troncal de banda ancha que conectaba once sitios regionales en todo Estados Unidos. Catorce líneas de fibra óptica de alta velocidad conectan sitios centrales tal y como se indica en la fig. 1.3, Seattle, Sunnyvale, Los Angeles, Denver, Kansas City, Houston, Chicago, Indianapolis, Atlanta, Nueva York y Washington, DC, su backbone cuenta con 13,000 millas de cable de fibra óptica y transferencia de unos 1.600 terabytes de datos al mes. [10][11][12]

LA vBNS también contribuye a Internet 2, conecta a varias instituciones gubernamentales y de investigación universitaria y en un principio sirvió como eje fundamental de Internet 2. Abilene y vBNS ahora se conectan entre sí, lo que permite a los usuarios de la red total conectividad a Internet 2. [14][15]

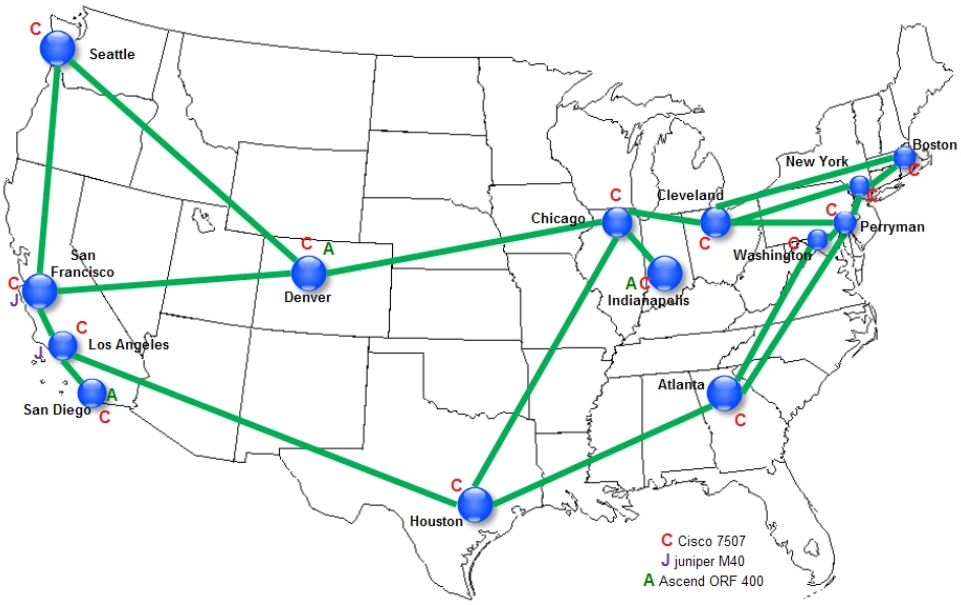

Fig. 1.2 Enlaces de Backbone vBNS, 1999. (Diagrama propio con referencia de [13])

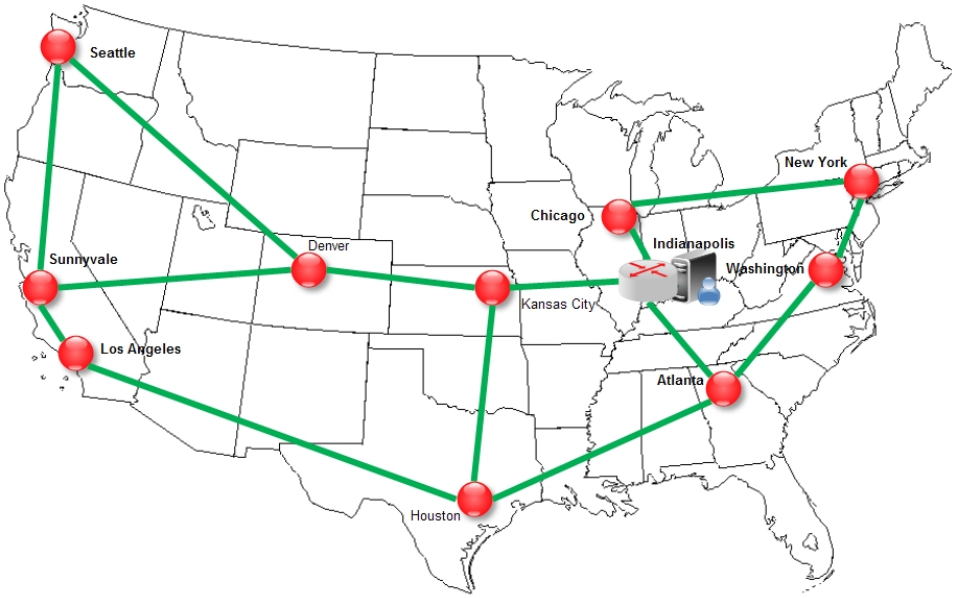

Fig. 1.3 Enlaces de Backbone Abilene, 2003 (Diagrama propio con referencia de [16] [17])

Para 2013 Internet 2 comprende 247 universidades de los EU., 78 empresas líderes, 70 miembros afiliados, incluidos los socios gubernamentales, 39 redes educativas regionales y estatales, más de 65 redes de investigación y educación de más de 100 países. [18]

La red Abilene o I2 utiliza el protocolo IP versión 6 (IPv6) la cual es compatible con IPv4 e implementa QoS (Quality of Service, Calidad del Servicio) además proporciona comunicación multicast. El backbone de Internet 2 tiene velocidades que superan los 2.4 Gbps, mientras que las conexiones de universidades al backbone de Internet 2 van de los 45 Mbps hasta los 622 Mbps. [19] [20]

1.4.1 Arquitectura I2

Internet 2 está compuesta por la red Abilene y la red vBNS como se muestra en la fig. 1.4, a los cuales se conectan los gigaPOPs (Gigabit Capacity Point of Presence, Punto de Presencia con Capacidad de Gigabits) que son nodos o centros de datos regionales que se encargan de la transferencia de grandes volúmenes de datos entre las redes regionales nacionales y redes internacionales, con un ancho de banda de T3.

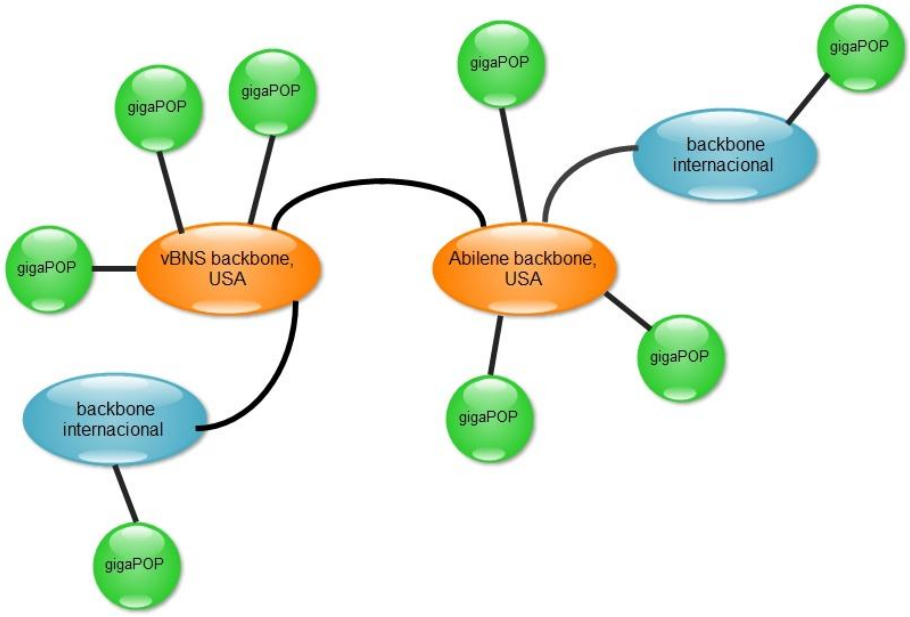

Fig. 1.4 Arquitectura genérica con gigaPOPs. (Diagrama propio con referencia de [21] [22])

Las conexiones entre gigaPOPs, vBNS o Abilene, campus y estaciones de trabajo se establecen de la siguiente manera: vBNS o Abilene a gigaPOP; gigaPOP a gigaPOP; gigaPOP a campus; estaciones de trabajo a campus.

Los gigaPOP se dividen en dos grupos, los gigaPOPs tipo 1: estos dan servicio solamente a miembros de Internet 2; gigaPOPs tipo 2: se encargan de dar servicio a miembros de Internet 2 como a otras redes, por ejemplo las internacionales. Los gigaPOP externos deben realizar una comunicación ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrona) a los centros gigaPOP para garantizar la calidad del servicio (QoS), mientras que para la comunicación interna entre gigaPOP se utiliza el protocolo IP. Los protocolos utilizados por los gigaPOP son IPv4, IPv6, OSPF, RIP, TCP/IP y BGP (Border Gateway Protocol).

GigaPOP a nivel lógico, es un centro regional de interconexión de red, que provee acceso a algunos miembros de Internet 2, este no pasa tráfico que no sea de Internet 2. Todo el tráfico IP va sobre ATM.

GigaPOP a nivel físico, es un lugar que alberga un conjunto de equipos de comunicaciones y hardware de soporte, este gigaPOP se encarga de gestionar la seguridad y servicios de Internet 2. [22] [23] [24]

Para 2013 el equipo con el que cuenta Internet 2 es: 7 routers juniper T-1600, 17 routers Juniper MX960, 21 Switches Juniper, 250 Racks, 15,717 millas de fibra oscura recién adquiridos, 8.8 Tbps de capacidad óptica, 100 Gbps de Capa 2 y Capa 3, 300 + Ciena ActiveFlex 6500 elementos de red y de acuerdo a la fig. 1.5 cuenta con 64 nodos distribuidos en todo Estados Unidos. [26]

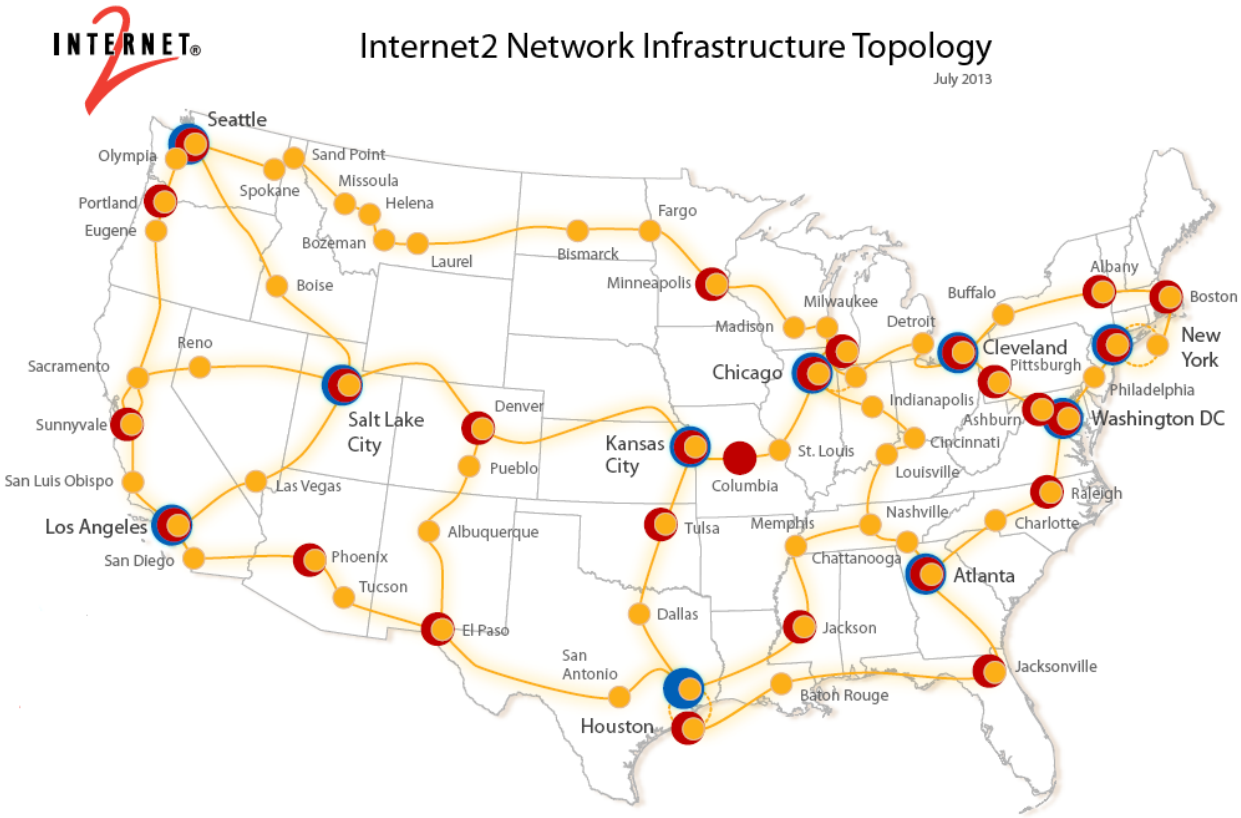

Fig. 1.5 Backbone de internet 2 (Abilene), con 64 nodos, Julio 2013. [27]

1.5 Otras Redes Avanzadas

En otras regiones del mundo se han creado redes de alta velocidad para integrar las redes de Internet 2, creadas en los Estados Unidos, el backbone Abilene ofrece conexiones con muchas redes de todo el mundo, como se muestra en la fig. 1.6.

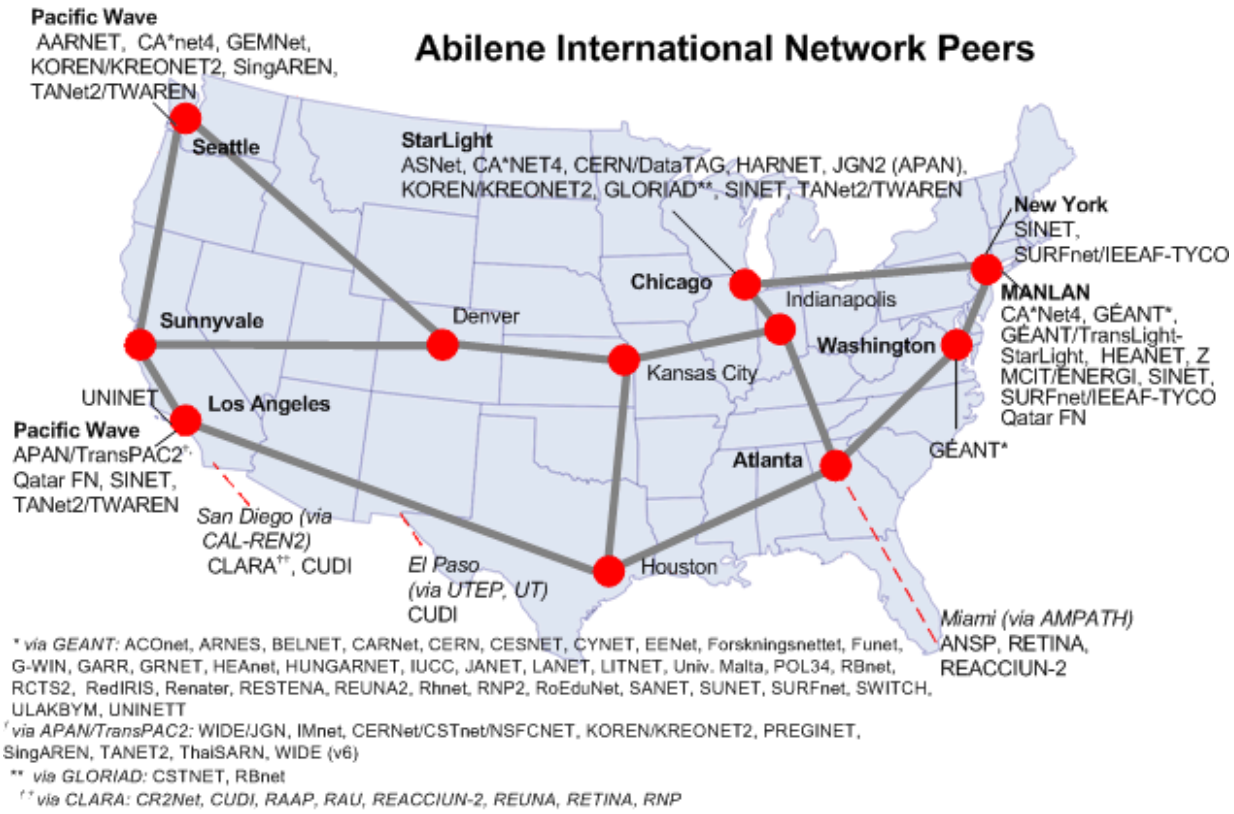

Fig. 1.6 Interconexión de internet 2 y otras redes del mundo, Julio 2013. (Internet 2) [28]

Los proyectos de redes de alta velocidad alrededor del mundo han servido para desarrollar nuevos proyectos de investigación en distintas materias e interconectar a las redes más avanzadas para el intercambio de información, principalmente buscan desarrollar nuevas tecnologías y su aplicación para transmitir grandes cantidades de información entre los miembros que las conforman, así mismo se crean grupos de trabajo para desarrollar y avanzar en las investigaciones que se realicen, En tabla 1.1 se muestran redes de Internet 2 creadas en el mundo. [28]

AMERICA						
RED	**Año de inicio**	**Interconexión**	**País**	**BW con I2 (Mbps)**	**BW interno**	**Referencia**
CANARIE	1993	Seattle (Pacific Wave/PNWGP)	Canada	3,000	10, 100Mbps	[29]
CLARA	2003	20 países de L.A.	L.A.	1, 2.5Gbps	622,155, 90, 45, 34Mbps	[33]
CEDIA			Ecuador			
CNTI			Venezuela			
CR2NET			Costa Rica			
CUDI		Houston	México	155/100		
REUNA		Atlanta (AMPATH/SFGP)	Chile	45		
RETINA		Atlanta (AMPATH/SFGP)	Argentina	45		
RNP [FAPESP]		Atlanta (AMPATH/SFGP)	Brasil	45		
SENACYT			Panamá			
CARIBNET	2012	Miami, 16 países	Caribe	300	45,155Mbps	[39]
ASIA PACIFICO						
AAIREP		Seattle (Pacific Wave/PNWGP)	Australia	2 x 155		
APAN	1997	Seattle (Pacific Wave/PNWGP)	Asia-Pacifico	622		[31]
CERNET, CSTNET, NSFCNET		Seattle (Pacific Wave/PNWGP)	China	622		
CAREN	2010	Asia central	Asia central		34Mbps	[35]
JAIRC		Sunnvale, New York	Japón	33, 2,500		
JUCC		Chicago	Hong Kong	45		
SingAREN		Sunnyvale	Singapur	155		
TEIN	2006	20 países mienbros	Eurasia		10, 45,155, 622Mbps, 1, 2.5, 10Gbps	[40][41]
NECTEC/UNINET		Los Ángeles	Thailandia	155		
TANet2		Seattle (Pacific Wave/PNWGP)	Taiwan	155		
ORIENTPLUS	2010		Europa/China		2x2.5Gbps	[36]
TERENA			Europa			
GEANT	2000	New York	Europa	3x10Gbps	1,2.5, 10Gbps, 155Mbps	[32]
AFRICA						
MCIT [EUN/ENSTINET]			Egipto			
TENET			Sudáfrica			
AFRICACONNECT	2011		África Meridional			[37]
EUROPA y MEDIO ORIENTE						
DANTE	1993	New york	Europa	7,500		[30]
DFN-Verein		New york	Alemania	7,500		
GARR		New york	Italia	7,500		
GIP-RENATER		New york	Francia	7,500		
Isrrael-IUCC			Israel			
RedIRIS			España			
RIPN		Chicago (via STAR-TAP-IPLS)	Rusia	155		
SANET			Eslovaquia			
JISC, UKERNA			Reino UNIDO			
EUMEDCONNECT		9 países miembros	Mediterráneo		45, 622Mbps	[38]

Tabla 1.1 Redes avanzadas, las redes sombreadas son las más importantes por su desarrollo.

1.6 Internet 2 en México

En México las universidades crearon un grupo llamado “CUDI” (Corporación Universitaria para el Desarrollo de Internet 2) para unirse a esta nueva internet, CUDI se creó el 8 de abril de 1999 y es el encargado de coordinar a Internet 2 en México. El objetivo de CUDI 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”* [42]

En 2013 CUDI cuenta con 266 instituciones miembros entre los que se encuentran Universidades, Institutos Tecnológicos, Centros Conacyt y Universidades Politécnicas. CUDI está formada por cuatro categorías miembros: Asociados Académicos, Afiliados Institucionales, Afiliados Académicos y Afiliados Empresariales, en la tabla 1.2 se muestran los asociados académicos. [43] [44] [45]

Asociados Académicos	
TELMEX	**AXTEL**
IPN	INSP
UAM	BUAP
UDLAP	UV
SEP	UAEMor
INTTELMEX	ILCE
ITESM-CEM-MTY	UAEH
UNAM	CONACYT
UNINET-VPNs	AVANTEL-VPNs
UDG	UAL
CICESE	UAT
UANL	
UACJ	

Tabla 1.2 Universidades miembros de CUDI. [45]

CUDI actualmente forma parte de la red CLARA (Cooperación Latino Americana de Redes Avanzadas) junto con otros países de América Latina para conectar a la comunidad científica de América con Europa, Asia, Norteamérica y el Pacífico.

1.6.1 INFRAESTRUCTURA CUDI

El backbone CUDI cuenta con una infraestructura de más de 8,000 km de enlaces aportados por Teléfonos de México (TELMEX) y AVANTEL (AXTEL), cada uno con 4,000 km, el cual cuenta con una velocidad de 155 Mbps. Esta red dorsal o Backbone permite la interconexión con redes académicas de Estados Unidos, Europa, Asia, América Latina y Oceanía. En la fig. 1.7 se muestra la arquitectura general de CUDI. [44]

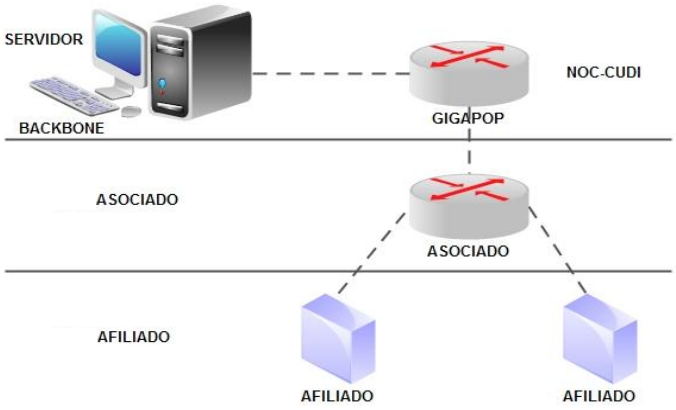

Fig. 1.7 Arquitectura general de CUDI. [47]

CUDI maneja cuatro jerarquías para Internet 2:

1. Enlaces internacionales Abilene, VBN, Cenic.
2. Nivel dorsal (SW y routers)
3. Nivel Asociados
4. Nivel afiliados

Enlaces internacionales: CUDI se conecta a Internet 2 vía enlaces físicos como se muestran en la tabla 1.3. [4]

Enlace Internacional	Lógico
Tijuana- Sn Diego California	Tijuana-San Diego supercomputer center
	Tijuana-Cenic
	Tijuana Abilene, Nodo Los Angeles
Cd. Juárez-El Paso TX	Cd Juárez-Abilene, Nodo Houston
Monterrey-Houston TX	Monterrey-VBNs, Nodo Houston

Tabla 1.3 Enlaces Internacionales a Internet 2. [4]

Nivel dorsal: es la infraestructura nacional con la que cuenta CUDI, como se muestra en la fig. 1.8.

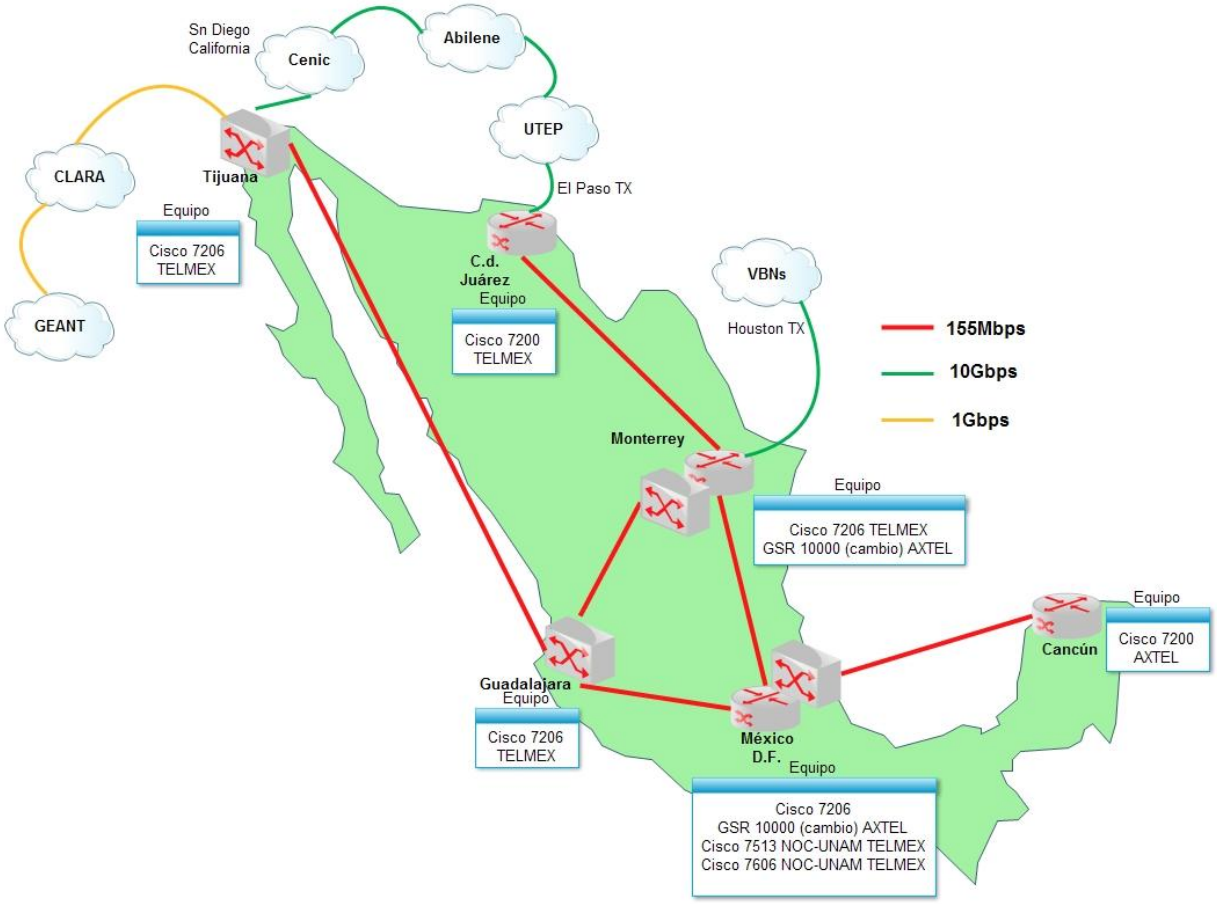

Fig. 1.8 Topología CUDI, con enlace DORSAL de STM-155 Mbps. (Diagrama propio con base en [4] [47])

Las velocidades que actualmente maneja CUDI son: El backbone integrado por México, Guadalajara, Monterrey, Tijuana, Cd. Juárez y Cancún cuenta con una velocidad de STM-1 (155 Mbps), los nodos asociados con una velocidad de 34 Mbps, mientras que los nodos afiliados de 2 Mbps.

Nivel asociado: cuenta con 22 enlaces asociados con una velocidad E3 en los nodos de agregación (11 TMX-9 AXTEL).

Nivel afiliados: administración de 22 conexiones de tránsito a redes académicas, más las que se han agregado.

En la fig. 1.9 se muestra el Backbone de CUDI el cual forma una topología de anillo con número de identificador de Sistema Autónomo (AS-18592), así como los principales miembros asociados y los enlaces internacionales con los que se conecta CUDI.

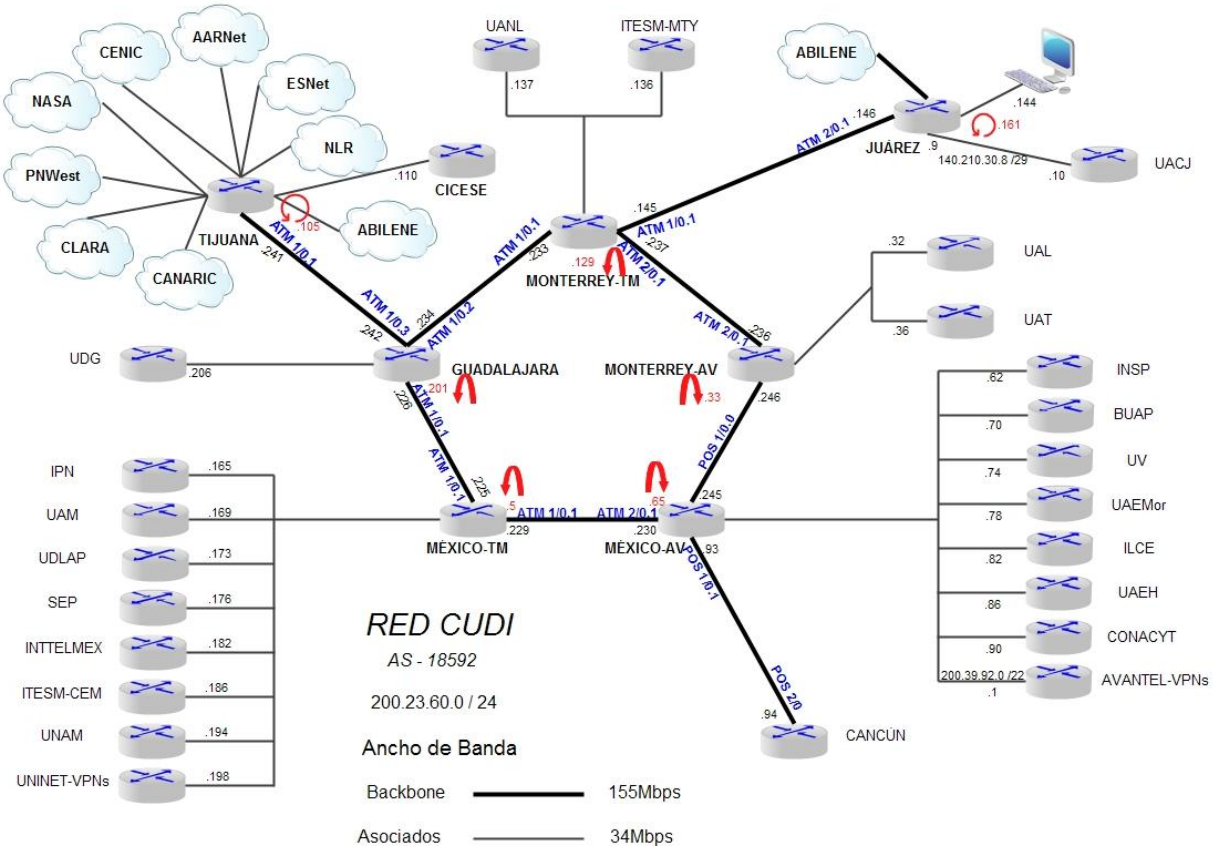

Fig. 1.9 Backbone de CUDI, 2013 (Diagrama propio con base en [48] [49]).

La infraestructura de la red CUDI cuenta con cuatro backbone: backbone TELMEX que cuenta con cinco nodos: México, Guadalajara, Monterrey, Cd. Juárez, Tijuana; backbone AXTEL cuenta con tres nodos: México, Monterrey, Cancún; backbone Bestel que conecta a San Antonio con México y la red IP-MPLS; backbone de la red NIBA (Red Nacional Para el Impulso de Banda Ancha) la cual se encuentra en 40 Ciudades del país, esta red conecta al usuario final físicamente a 1Gbps y está limitada a 100 Mbps, su acceso a la red dorsal es de 1 Gbps hasta 10 Gbps, en la fig. 1. 10 se muestran los cuatro backbone de la red CUDI. [42] [50] [51]

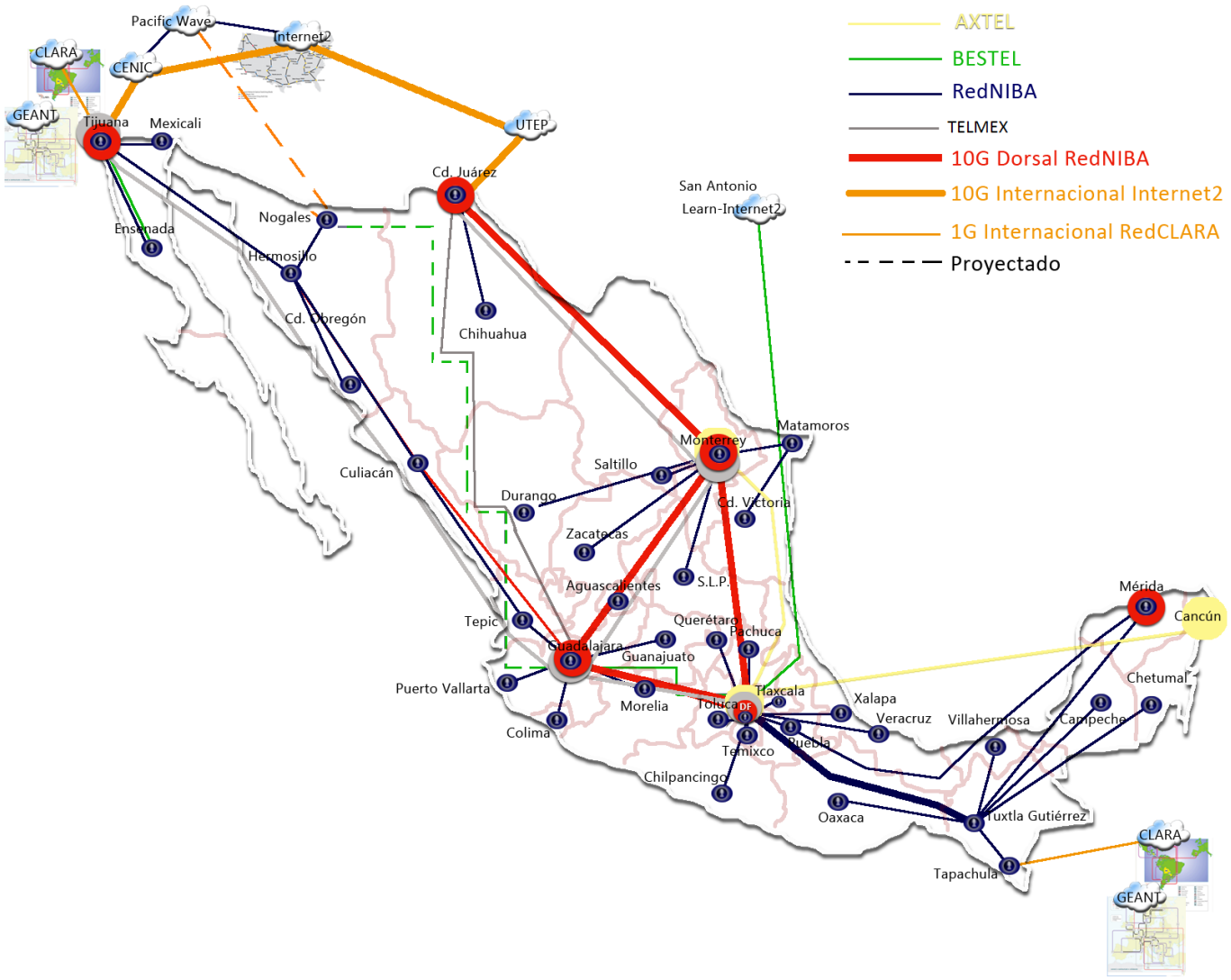

Fig. 1.10 Topología de la Red CUDI completa con 4 Backbone, 24 de Octubre 2013. [48]

CUDI incorpora los más avanzados protocolos en redes de datos, es capaz de soportar IPv6, H.323, OSPF, QoS, Multicast, MPLS y HDTV, para poder conectarse a estas redes de alta velocidad y dentro de ella lo que permite desarrollar aplicaciones en astronomía, ecología, supercómputo, matemáticas, salud, medicina, laboratorios, bibliotecas digitales y medios estudiantiles. [52]

1.6.2 NOC CUDI

El NOC-CUDI se encuentra en la Ciudad de México en las instalaciones de la UNAM, el NOC-CUDI se encarga de la administración, control, monitoreo y operación de toda la infraestructura física y lógica que conforma la red dorsal para asegurar el óptimo desempeño de la red, las funciones de NOC-CUDI son:

1. Monitoreo: se encarga de la detección de fallas verificando las alarmas provenientes de los equipos y realiza pruebas preliminares.
2. Ingeniería: se encarga de revisar los detalles técnicos de los protocolos de cada equipo que conforma el backbone.
3. Operación/Soporte: encargado de la infraestructura lógica y física del NOC-CUDI.
4. Análisis/configuración: su función es la de revisar los desempeños de los equipos, seguridad, topología, tecnologías emergentes y normatividad.
5. Administración de software: se encarga de revisar los sistemas operativos, programas y software con el que cuenta el NOC-CUDI.
6. Atención y seguimiento de fallas: se encarga del seguimiento y resolución de fallas. [4] [52]

Su infraestructura cuenta con 1 router Cisco 7206 en Cd. Juarez, 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), SW de 12 puertos 100/1000 UTP y 3 PC [tres personas: 2 CUDI y 1 UNAM] esto hasta el 2007. [52]

Capítulo 2

Protocolos de Enrutamiento

En este capítulo se presentan los protocolos de enrutamiento utilizados por los equipos llamados routers, estos interconectan dos o más redes, eligiendo el mejor camino para poder reenviar paquetes. Primeramente se da la definición de enrutamiento, posteriormente se describe brevemente el funcionamiento del algoritmo de enrutamiento, en seguida se presentan los protocolos de enrutamiento: RIP, RIPv2, IGRP, EIGRP, OSPF e IS-IS y cada una de sus características. Cabe mencionar que el protocolo de enrutamiento OSPF es el empleado por la red CUDI.

2.1 Algoritmos de enrutamiento

El enrutamiento es un proceso en el que los datos son enviados de una ruta a otra ruta, el dispositivo que se encarga de realizar esta función es el router el cual trabaja en la capa 3 o capa de red del modelo ISO-OSI, (International Organization for Standardization - Open System Interconnection). Un router realiza dos funciones, el enrutamiento y el switching. El enrutamiento se da cuando aprende y mantiene la topología de la red a través de su tabla de ruteo, el switching se da cuando realiza un movimiento real del tráfico desde una interfaz de entrada a una interfaz de salida.

Para poder enviar paquetes desde una red LAN hacia otra red LAN o MAN o viceversa se lleva a cabo un proceso de enrutamiento el cual se apoya en los protocolos de enrutamiento, los cuales a su vez son ayudados por los algoritmos de enrutamiento.

Un algoritmo de enrutamiento es aquel que se encarga de decidir la ruta que seguirán los datos para llegar a su destino. Estos se basan en métricas, como el número de saltos, el ancho de banda, el retraso, la carga, la fiabilidad o el tiempo. [53]

Los algoritmos de enrutamiento cumplen con las siguientes propiedades: corrección, sencillez, robustez, estabilidad, equitatividad, optimalidad. Existen dos clases de algoritmos de enrutamiento:

- ✓ Algoritmos no adaptables: no basan sus decisiones de enrutamiento con mediciones o estimaciones de tráfico, tampoco reflejan los cambios en su topología.
- ✓ Algoritmos adaptables: cambian sus decisiones de enrutamiento para reflejar los cambios de topología y el tráfico.

Dos de los algoritmos más utilizados son Dijkstra y Bellman-Ford. [54] [55]

2.2 Protocolos de enrutamiento

Los protocolos de enrutamiento se dividen en dos tipos, IGP (Interior Gateway Protocol, Protocolo de Gateway Interior) y EGP (Exterior Gateway Protocol, Protocolo de Gateway Exterior). Estos son protocolos de áreas, que se llaman también dominios de enrutamiento, los dominios de enrutamiento se conocen como AS (Autonomous System, Sistemas Autónomos) que son una colección de redes controladas por una sola autoridad administrativa y técnica.

Un protocolo de gateway interior (IGP): es un protocolo de enrutamiento que se utiliza para seleccionar la mejor ruta e intercambiar información dentro de un AS, ejemplos de esos protocolos intradominios son: RIP (Routing Information Protocol, Protocolo de Información de Enrutamiento), RIPv2 (Routing Information Protocol version 2, Protocolo de Información de Enrutamiento versión 2), OSPF (Open Shortest Path First, Primero la Ruta más Corta), IGRP (Interior Gateway Routing Protocol, Protocolo de Enrutamiento de Gateway Interior), EIGRP (Enhanced Interior Gateway Routing Protocol, Protocolo de Enrutamiento de Gateway Interior Mejorado), e IS-IS (Intermediate System to ntermediate System, Sistema Intermedio a Sistema Intermedio).

Un protocolo de gateway exterior (EGP): es un protocolo de enrutamiento que se encarga de seleccionar la mejor ruta para intercambiar información entre distintos AS, ejemplos de estos protocolos son: EGP (Exterior Gateway Protocol, Protocolo de Gateway Exterior) el cual se encuentran definido en el RFC904 y el BGP (Border Gateway Protocol, Protocolo de Gateway de Frontera) definido en el RFC1105 y RFC1771. [56] [57] [58] [59] [60]

Los IGP y EGP son fundamentales para todas las redes que se requieren diseñar ya que la internet está subdividida en sistemas autónomos, los cuales pueden ser administrados independientemente. Así los routers dentro de un AS se comunican por medio de un IGP y los routers de frontera se comunican mediante BGP como se muestra en la fig. 2.1.

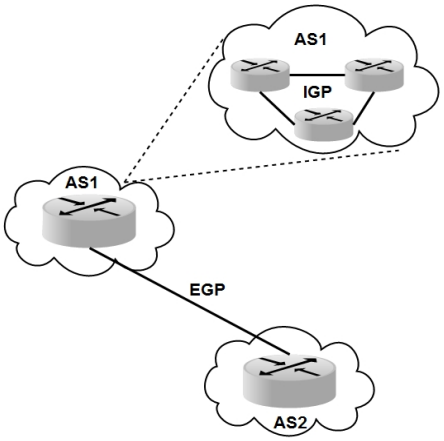

Fig. 2.1. Protocolos IGP y EGP utilizados por los AS (Diagrama propio).

Tanto los IGP como los EGP se clasifican en dos tipos de protocolos de ruteo, aquellos que tienen clase y los que no tienen clase. Los que tienen clase se llaman así porque utilizan direcciones de red clase A, B o C pero no utilizan información de la máscara de subred por lo que no admiten VLSM (Variable Length Subnet Masks, Máscaras de Subred de Longitud Variable), los protocolos RIP v1 e IGRP son de este tipo. Los protocolos sin clase son aquellos que admiten la dirección de red y la máscara de subred, están diseñados para contrarrestar algunas limitaciones de los protocolos con clase, pueden soportar VLSM, ejemplos de este tipo de protocolos son RIP v2, OSPF, EIGRP, IS–IS, BGP. [61] [62]

Los protocolos IGP y EGP utilizan tablas llamadas “tablas de ruteo” que se utilizan para almacenar información en la memoria RAM de los routers, las cuales contienen información sobre la ruta de redes remotas y las redes conectadas directamente para seleccionar la mejor ruta para alcanzar un destino. La tabla de ruteo está compuesta por 7 elementos: protocolo de ruteo, la red o subred lógica, distancia administrativa, valor métrico, dirección lógica del próximo salto, tiempo de la actualización o ejecución e interfaz a través de la cual se conoció la ruta. La fig. 2.2 muestra un ejemplo de la tabla de ruteo. [62]

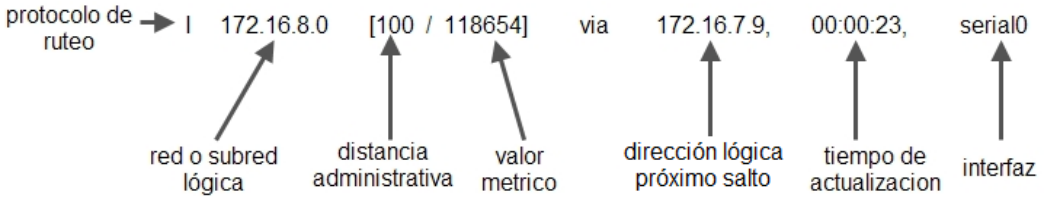

Fig. 2.2. Ejemplo de Componentes de la Tabla de Ruteo. [62]

A. Protocolo de ruteo: es el tipo de protocolo IGP utilizado.

B. Red o subred lógica: es la dirección de red destino que se quiere alcanzar.

C. Distancia administrativa: se utiliza como identificador de los protocolos de enrutamiento, se utiliza como medida de fiabilidad del origen de la información, la tabla 2.1 presenta las distancias administrativas predeterminadas.

Origen de la Ruta	Distancia Administrativa Predeterminada
Interfaz conectada	0
Ruta estática fuera de una interfaz	0
Ruta estática de un próximo salto	1
Ruta de resumen de EIGRP	5
BGP externa	20
EIGRP interna	90
IGRP	100
OSPF	110
IS – IS	115
RIP (v1 y v2)	120
EGP	140
EIGRP externa	170
BGP interna	200
Desconocido	255

Tabla 2.1. Distancias Administrativas. [62]

D. Valor métrico: La métrica es un valor que se utiliza para determinar la distancia para llegar al destino, la mejor ruta o camino es el que cuenta con la métrica más baja, las métricas son: conteo de saltos, ancho de banda, el coste de la comunicación, el retraso, la carga, el coste de la ruta y la fiabilidad, los cuales son utilizados por los protocolos de ruteo. [61] [62]

E. Dirección lógica del próximo salto: es la dirección del dispositivo siguiente, en la ruta hacia el destino.

F. Tiempo de la actualización o ejecución: es el tiempo de actualización de la tabla de enrutamiento la cual depende del protocolo de enrutamiento utilizado.

G. Interfaz: es la interfaz física por donde se envían y reciben paquetes.

A continuación se describen términos que emplean los protocolos de enrutamiento:

Equilibrio de carga: es cuando se comparte tráfico de paquetes por múltiples rutas.

A. Equilibrio de carga iguales: es cuando dos o más rutas tienen la misma métrica y el mismo costo, esas rutas serán compartidas.
B. El equilibrio de cargas desiguales: es cuando se utilizan diferentes métricas y distinto costo.

Convergencia: es cuando todos los routers de la red están sincronizados y tienen información completa sobre la red aún si se producen cambios en su topología.

Escalabilidad: se da cuando una red se expande y depende del protocolo de enrutamiento utilizado.

2.2.1 IGP: RIP

RIP (Routing Information Protocol, Protocolo de Información de Enrutamiento), es un protocolo de enrutamiento desarrollado por Xerox Network System en 1982, que se utiliza para seleccionar o localizar la mejor ruta para alcanzar su destino ubicado en la misma red, RIP es un Protocolo de Gateway Interior y se encuentra definido en el RFC 1058 y el RFC 1388 actualizado. RIP calcula la distancia del origen al destino por medio de la métrica de número de saltos, es decir, cuántos routers debe atravesar

un paquete para llegar a su destino final, también actualiza sus tablas de ruteo cada 30 s. RIP evita la cuenta al infinito mediante un límite de saltos, el número máximo de saltos en una ruta es de 15, por lo que si llega a 16 saltos el destino es inalcanzable, ver fig. 2.3. [63] [64] [65]

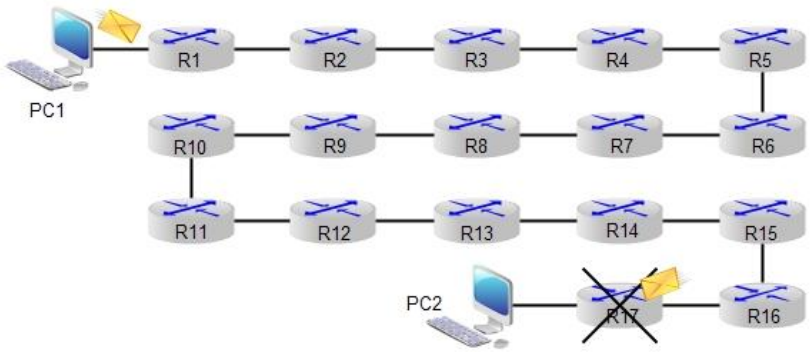

Fig. 2.3. Destino inalcanzable de PC1 a PC2 utilizando RIP (Diagrama propio).

RIP utiliza el algoritmo Bellman-Ford, en el caso que existan múltiples rutas al destino se selecciona la que tenga el menor número de saltos, como se muestra en la fig. 2.4.

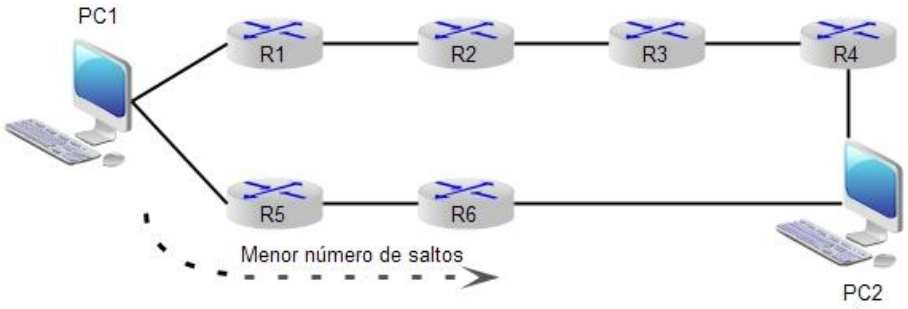

Fig. 2.4. Ruta con menor número de saltos (Diagrama propio).

Una de las desventajas de RIP es que se conecta constantemente con los router vecinos para actualizar su tabla de enrutamiento.

Características:

1. Algoritmo de enrutamiento por vector distancia (Bellman-Ford).
2. Métrica número de saltos, número máximo de saltos 15. Si el número de saltos es superior a 15 el destino es inalcanzable.
3. Se actualiza cada 30 s.
4. Pertenece a los protocolos con clase.
5. Admite balanceo de carga hasta seis rutas del mismo costo.
6. No admite autenticación. [66] [67]

La fig. 2.5 muestra el formato del paquete RIP el cual contiene nueve campos:

C1	C2	C3	C4	C5	C6	C7	C8	C9
1-octet Command field	1-octet Version number field	2-octet zero field	2-octet AFI field	2-octet zero field	4-octet IP address field	4-octet zero field	4-octet zero field	4-octet metric field

Fig. 2.5. Campos de RIP v1. [64]

Campo 1: Comando: indica si el paquete es una solicitud o una respuesta.

Campo 2: Número de versión: especifica la versión de RIP utilizada v1 o v2.

Campo 3, 5, 7, 8: Zero: Este campo no se utiliza realmente en el RFC 1058 RIP, sólo fue añadida con el objeto de facilitar la compatibilidad con las diferentes versiones de RIP.

Campo 4: Identificador de dirección familiar (AFI): especifica la familia de los protocolos utilizados como IP al cual le corresponde el AFI 2.

Campo 6: Dirección IP: especifica la dirección IP utilizada.

Campo 9: Métricas: indica el número de saltos entre redes (routers) que han atravesado los paquetes para llegar a su destino. Este valor es entre 1 y 15 para una ruta válida, o 16 para una ruta inalcanzable.

2.2.2 IGP: RIP v2

El protocolo RIP v2 es una mejora de RIP v1 la cual se realizó en 1994, está definido en el RFC 1723, RIP v2 proporciona un mecanismo de autentificación simple que no es compatible con RIP v1. [68]

Características de RIP v2:

1. Algoritmo de enrutamiento por vector distancia (Bellman-Ford).
2. Métrica número de saltos, número máximo de saltos 15, Si el número de saltos es superior a 15 el destino es inalcanzable.
3. Se actualiza cada 30 s.
4. Pertenece a los protocolos sin clase, soporta máscaras de longitud variable (VLSM).
5. Admite balanceo de carga hasta seis rutas del mismo costo.
6. Tiene mecanismos de autenticación para seguridad en las tablas de ruteo. [68] [69] [70] [71]

La fig. 2.6 muestra el formato del paquete RIP v2 el cual contiene nueve campos:

C1	C2	C3	C4	C5	C6	C7	C8	C9
1-octet Command field	1-octet Version number field	2-octet Unused field	2-octet AFI field	2-octet Route tag field	4-octet Network address field	4-octet Subnet mask field	4-octet Next hop field	4-octet metric field

Fig. 2.6. Campos de RIP V2. [69]

C1: Comando: indica si el paquete es una solicitud o una respuesta.

C2: Número de versión: especifica la versión de RIP utilizada.

C3: No utilizado: este campo tiene un valor de cero.

C4: Identificador de dirección familiar (AFI): especifica la familia de los protocolos utilizados como IP al cual le corresponde el AFI 2, si la AFI contiene un mensaje para 0xFFFF, contiene información de autenticación.

C5: Ruta tag: proporciona un método para distinguir entre las rutas internas aprendidas por RIP y rutas externas aprendidas de otros protocolos.

C6: Dirección IP: especifica la dirección IP utilizada.

C7: Máscara de subred: contiene la máscara de subred de 32 bits.

C8: Siguiente salto: se usa para identificar una dirección de siguiente salto mejor que la del router emisor, si el campo está en (0.0.0.0) la dirección del router emisor es la mejor dirección de siguiente salto.

C9: Métricas: indica el número de saltos entre routers.

2.2.3 IGP: IGRP

IGRP (Interior Gateway Routing Protocol, Protocolo de Enrutamiento de Gateway Interior) es un protocolo desarrollado por CISCO en 1985, este protocolo solventa algunas de las limitaciones de RIP v1, IGRP lleva un registro de las rutas preferidas hacia un destino las cuales se encuentran en su tabla de ruteo, si la ruta no se encuentra debe de esperar una actualización para que el paquete pueda llegar a su destino. Actualmente se considera obsoleto. Las características de IGRP son: [72] [73] [74] [75]

1. Algoritmo de enrutamiento por vector distancia (Bellman Ford).
2. Utiliza “métrica compuesta” por ancho de banda de 1200 bps hasta 10 Gbps, retardo con un valor de 1 hasta 224, la carga con un valor de 1 hasta 125, la confiabilidad con un valor de 1 hasta 125, número de saltos por defecto 100 o se puede establecer de 1 hasta 255.
3. Actualizaciones cada 90 s, si no recibe ninguna actualización durante 270 s la ruta es inalcanzable y después de 630 s se elimina la ruta de la tabla de ruteo.
4. Pertenece a los protocolos con clase.

2.2.4 IGP: EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol, Protocolo de Enrutamiento de Gateway Interior Mejorado) es un protocolo desarrollado por CISCO en 1992, EIGRP es la versión mejorada de IGRP, utiliza el protocolo RTP (Reliable Transport Protocol, Protocolo de Transporte Confiable) para la entrega confiable y no confiable de paquetes, también garantiza rutas sin bucles por medio de su algoritmo DUAL (Diffusing Update Algorithm, Algoritmo de Actualización por Difusión). [76] [77]

EIGRP utiliza cinco tipos de paquetes:

- ✓ Paquetes HELLO: se utiliza para el descubrimiento de redes.
- ✓ Paquetes de actualización: se utiliza cuando se descubre una nueva ruta y cuando se completa la convergencia.
- ✓ Paquete consulta: se utiliza para buscar un sucesor factible al destino.
- ✓ Paquetes respuesta: se envía como repuesta a un paquete de consulta.
- ✓ Paquetes ACK: se utiliza para confirmar las actualizaciones.

Sus principales características son:

1. Algoritmo de enrutamiento por vector distancia y link state. Utiliza el algoritmo DUAL para una convergencia rápida.
2. Utiliza métricas compuesta por ancho de banda, retardo, la carga y la confiabilidad.
3. No existen actualizaciones periódicas, sólo se envían actualizaciones cuando hay cambios en la topología de la red. Utiliza el protocolo HELLO, para descubrimiento y actualizaciones de redes.
4. Tiempo de espera de un paquete HELLO es de 15 s, si expira el destino es inalcanzable y se buscará una nueva ruta.
5. Pertenece a los protocolos sin clase. Soporta VLSM.
6. Soporta el protocolo RTP.

La distancia administrativa (AD) de EIGRP es de 90 para rutas internas y de 170 para rutas externas las cuales están predeterminadas. EIGRP puede autentificar la información de enrutamiento esto garantiza que sólo los routers que están configurados con la misma contraseña acepten información de enrutamiento de otros routers, este protocolo de enrutamiento puede equilibrar la carga por múltiples rutas con diferentes métricas hasta un balanceo de carga de cuatro rutas de coste equivalente. [76] [78]

2.2.5 IGP: OSPF

OSPF (Open Shortest Path First, Primero la Ruta más Corta) fue desarrollado en 1988 por IETF (Internet Engineering Task Force), se encuentra definido en el RFC 1247, es un protocolo IGP por lo que se utiliza para conectar redes dentro de un AS [79]. OSPF utiliza el algoritmo "*Link state*" para crear un mapa de la topología de la red, para lo cual utiliza el paquete Hello para descubrir cualquier "*vecino*" en sus enlaces y establecer una relación. Un vecino es un router que utiliza el mismo protocolo de enrutamiento, la métrica se define en el RFC 2328 la cual es un valor arbitrario llamado costo, su métrica de costo más utilizada es el ancho de banda. [80] [81]

OSPF utiliza el concepto de áreas que son un conjunto de redes y routers que tienen una misma identificación, estas crean un diseño jerárquico en las redes, lo cual permite una mejor identificación de problemas. Las áreas son una subdivisión de áreas más pequeñas, esto ayuda a mejorar el rendimiento de la red debido a que cada área ejecuta su propio algoritmo SPF. OSPF contiene dos niveles de áreas el área 0 o de backbone y las áreas restantes, los router localizados en el área 0 son nombrados de backbone, los routers que delimitan el área 0 con las demás áreas se llaman ABR (Area Border Routers, Routers de Frontera entre Áreas). Los routers ASBR (Autonomous System Boundary Routers, Routers de Frontera entre Sistemas Autonomos) conectan a otros AS los cuales pueden tener otros protocolos de enrutamiento, este se encuentra ubicado en el área 0. Los routers IR (Internal router,

Routers Internos) son los que se encuentran dentro de las diferentes áreas de OSPF. [82]

En la fig. 2.7 se muestra el AS1 el cual utiliza el protocolo OSPF para cada una de sus tres áreas, también se muestran los nombres de cada uno de los routers que intervienen en las áreas de OSPF.

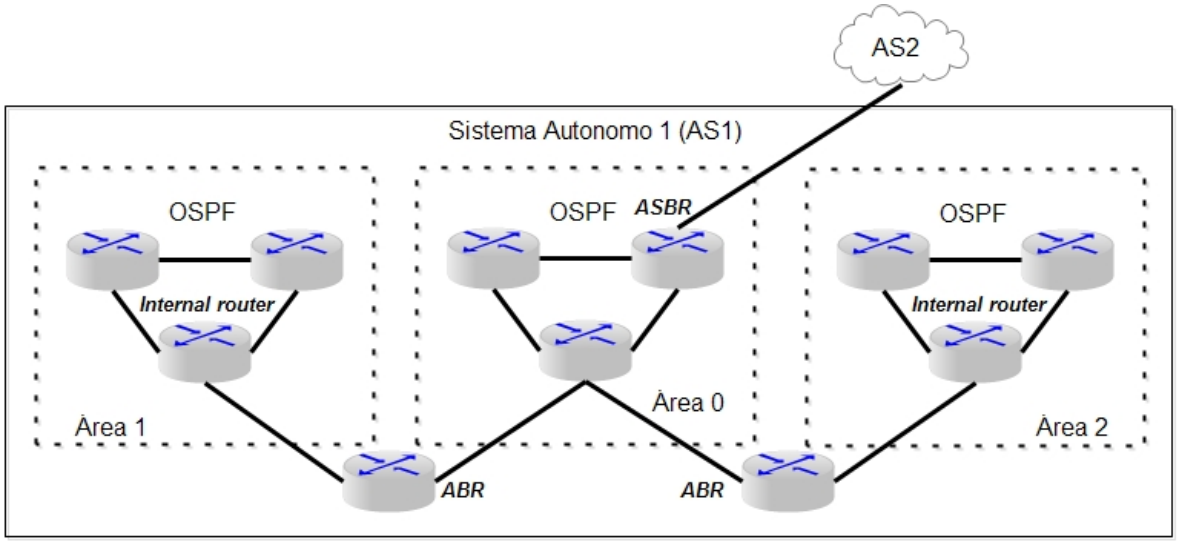

Fig. 2.7. Tres áreas dentro de un AS1 utilizando el protocolo OSPF (Diagrama propio).

OSPF utiliza cinco tipos de paquetes (LSP, Link State Paquet) para el proceso de enrutamiento:

1. HELLO: se utiliza para el descubrimiento de redes e indica si se encuentra activo, se envían paquetes Hello cada 10 s.
2. DBD (Database Descriptor, Descriptores de Base de Datos): se utiliza para comparar los link state de los routers emisores con los de routers receptores.
3. LSR (Link State Request, Solicitud de Estado de Enlace): se utiliza para pedir información de la DBD, la cual es utilizada por los router receptores.
4. LSU (Link State Update, Actualización de Estado de Enlace): se utiliza para responder los LSR y anunciar nueva información.
5. LSAck (Link State Acknowledgements, Acuse de recibo de Estado de Enlace): se utiliza para confirmar la llegada de LSU.

OSPF establece a sus vecinos de la siguiente manera: primero determina si hay otros vecinos que cuenten con este protocolo en sus enlaces; segundo, se envían paquetes "*Hello*" a todas las interfaces que tienen OSPF, los culés son confirmados; tercero, se establece una relación con el vecino para intercambiar paquetes "*Hello*". En la fig. 2.8 se muestra él envío de paquetes *Hello* para el descubrimiento de sus vecinos.

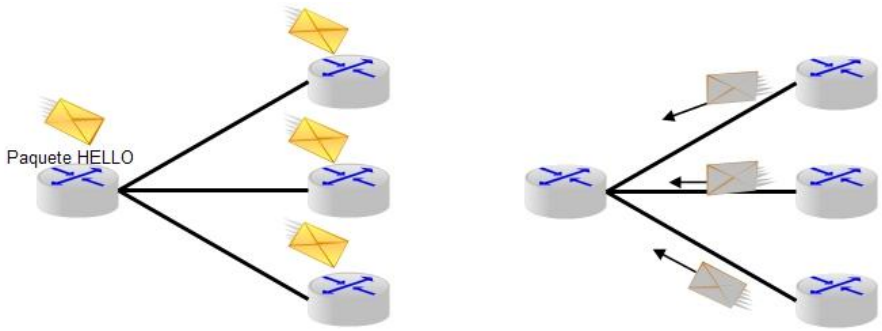

Fig. 2.8. Paquete Hello para descubrir vecinos (Diagrama propio).

Finalmente cada router crea una base de datos a partir del LSA (Link State Advertisements, Anuncios de Estado de Enlace), esta base de datos la usa el algoritmo Dijkstra para crear un árbol SPF el cual se utiliza para completar la tabla de enrutamiento, como se muestra en la fig. 2.9.

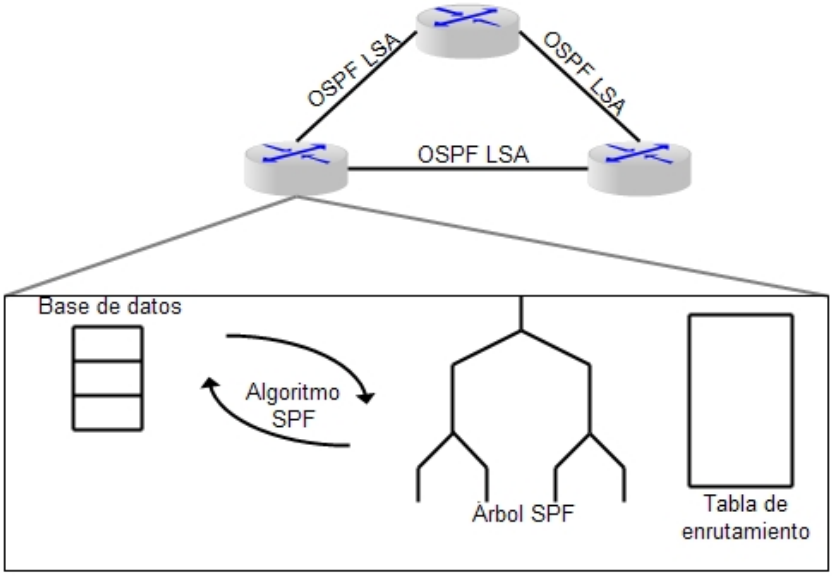

Fig. 2.9. Pasos que realiza OSPF para obtener la tabla de enrutamiento. [83]

Posteriormente se selecciona un DR (Designate Router, Router Designado) el cual es el responsable de las actualizaciones de los routers si la red llegara a cambiar, también selecciona un BDR (Backup Designated Router, Router Designado de Respaldo), el cual es el encargado de supervisar al DR y de reemplazarlo en caso de falla.

El router que tiene el valor de prioridad más alto es el DR, en tanto el segundo router con valor de prioridad alto es el BDR, el valor de prioridad es configurado por un administrador. El valor máximo de prioridad que puede tomar es de 255, en la fig. 2.10 se muestra la elección del DR y BDR. [84]

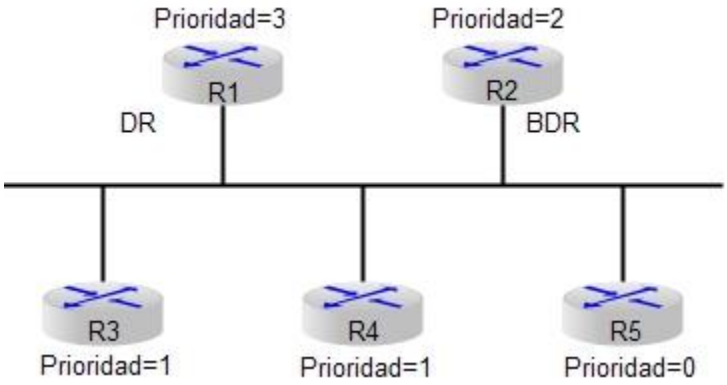

Fig. 2.10. Elección de DR=R1 con valor de prioridad = 3 y BDR=R2 con valor de prioridad = 2. [84]

OSPF determina el cálculo del costo de la ruta con la ecuación (2.1), tal valor obtenido se usa como métrica y se prefiere el costo menor:

$$costo = \frac{10^8}{BW} \tag{2.1}$$

donde:

10^8 : en bps.

$costo$: es el costo de un enlace OSPF.

BW : es el ancho de banda del enlace en bps.

En la tabla 2.2 se presentan los diferentes costos de los diferentes tipos de enlace que suele utilizar OSPF. [85]

Tipo de interfaz	Costo
Fast Ethernet	1
Ethernet	10
E1	48
T1	64
128kbps	781
64kbps	1562
56kbps	1785

Tabla 2.2. Costos de los diferentes tipos de interfaz. [84]

OSPF cuenta con autentificación y encriptación de su información de enrutamiento, lo cual garantiza que los router sólo pueden aceptar información de enrutamiento de otros router que cuenten con la misma contraseña o información de autentificación, el algoritmo utilizado para la autenticación es MD5 (Message Digest 5) el cual genera un número de encriptación que es utilizado por los routers, la autentificación previene que los routers reciban información falsa de otros routers. [86]

Características:

1. Algoritmo de enrutamiento por link state (Dijkstra).
2. La métrica utilizada es el ancho de banda, la distancia administrativa predeterminada es de 110.
3. Actualizaciones cada 30 s, para sincronización de los routers.
4. Pertenece a los protocolos sin clase. Soporta VLSM.
5. Admite balanceo de carga hasta seis rutas del mismo costo.
6. Cuenta con autentificación. [81] [86] [87]

El formato del paquete OSPF contiene nueve campos en su cabecera la cual tiene 24 bytes y 4 bytes del campo Data, como se muestra en la fig. 2.11:

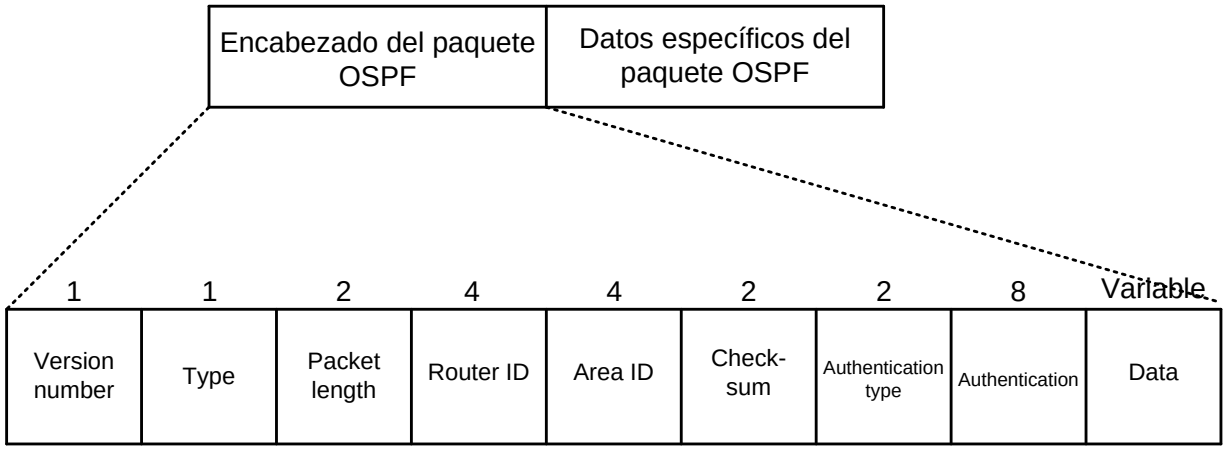

Fig. 2.11. Campos de la cabecera de OSPF. [80]

Donde:

- ✓ Número de versión: identifica la versión de OSPF utilizada.
- ✓ TIPO: tipo de paquete OSPF, HELLO (1), DBD (2), LS solicitud (3), LS actualización (4), ACK (5).
- ✓ Longitud del paquete: especifica la longitud del paquete.
- ✓ ID del Router: identificador del router origen, identifica el origen del paquete.
- ✓ ID del área: especifica el área desde donde se originó el paquete.
- ✓ Checksum: comprueba el contenido del paquete, por los errores que sufriera durante el transporte.
- ✓ Tipo de autenticación: contiene el tipo de autenticación y se puede configurar por área, el tipo 0 indica que no hay autenticación, el tipo 1 indica autenticación.
- ✓ Autenticación: contiene información de autentificación.
- ✓ Dato: contiene información de encapsulamiento de capas superiores.

El formato de paquetes de hello OSPF está formado por los campos que se muestran en la fig. 2.12:

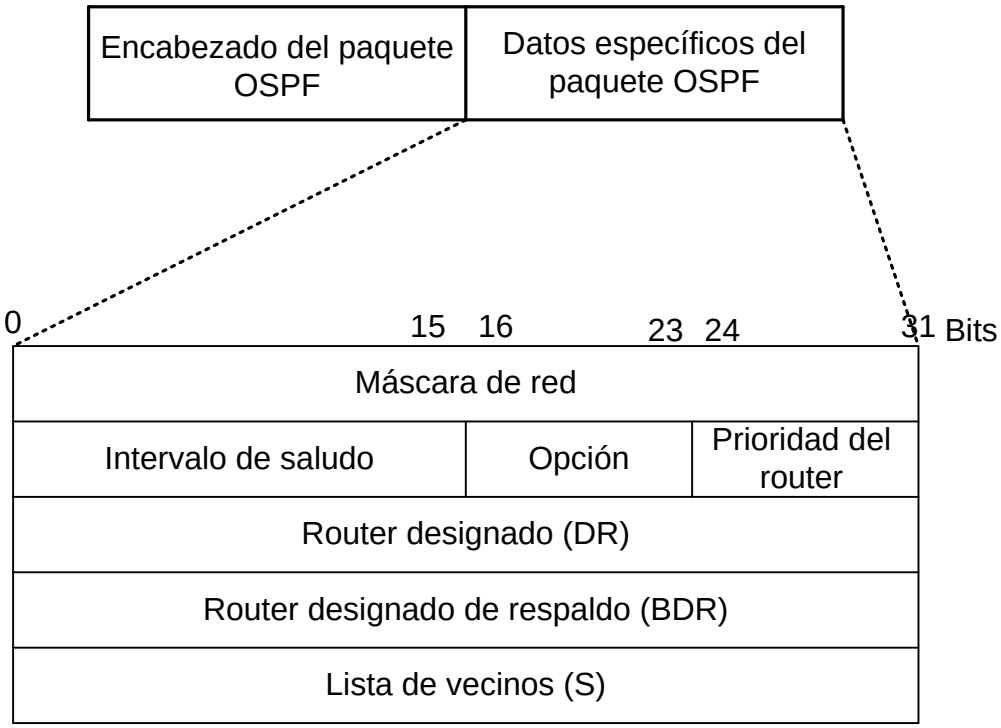

Fig. 2.12. Campos Hello de OSPF. [86]

Donde:

- ✓ Máscara de red MSK: máscara de subred asociada con la interfaz de envió.
- ✓ Intervalo Hello: tiempo de envió de saludos entre routers en segundos.
- ✓ Prioridad del router: selecciona el DR o BDR.
- ✓ Router designado (DR): identificador del router designado.
- ✓ Router designado de respaldo (BDR): identificador del router de respaldo.
- ✓ Lista de vecinos: enumera a los routers vecinos con los que se ha establecido una comunicación.

Existen otras versiones de OSPF tales como OSPF v2 que se desarrolló en 1991, y se definió en el RFC 2328 para redes IPv4, mientras que OSPFv3 se desarrolló en 1999 y se definió en el RFC 2740 para redes IPv6. [88] [89]

2.2.6 IGP: IS-IS

IS-IS (Intermediate System to Intermediate System, Sistema Intermedio a Sistema Intermedio) fue desarrollado por ISO (Organización Internacional para la Estandarización) se encuentra definido en ISO 10589 y en el RFC 1195, IS-IS es utilizado principalmente por los proveedores de servicio de Internet (ISP), al igual que OSPF, IS – IS utiliza el protocolo HELLO para descubrir a sus vecinos, estos forman una relación para intercambiar sus bases de datos y sincronizarse, sólo que IS-IS se ejecuta en la capa de enlace de datos. Su métrica utilizada es el costo que puede ser asignada o se puede calcular utilizando características del enlace. [90]

En IS-IS, un router es definido como un sistema intermedio (IS) y un host como un sistema final (ES).

IS-IS se divide en áreas, pero todas estas áreas no requieren que estén conectas al area 0, esta jerarquía se divide típicamente en un nivel de Backbone (nivel 2) y otro subnivel de áreas (nivel 1), un router puede estar dentro del nivel 1, nivel 2 o dentro del nivel 1-2.

Nivel 1: intra-área no saben nada fuera de su topología, sólo conoce la información de su área, por ejemplo cuando los routers se conectan dentro de un area, es decir sería el equivalente al IR en OSPF.

Nivel 2: inter-área conocen la topología fuera de sus áreas, pero no conocen nada de la topología dentro de las áreas, por ejemplo cuando los routers conectan dos o más áreas, sería el equivalente al ABR en OSPF.

Nivel 1-2: puede hacer funciones tanto de nivel 1 como de nivel2, a su vez se puede conectar con otros AS, sería el equivalente a los ASBR en OSPF.

Este tipo de jerarquía permite la escalabilidad y reducir las tablas de enrutamiento de las áreas. En la fig.2.13 se muestran los niveles 1, 2 y 1-2 dentro de tres áreas de IS-IS.

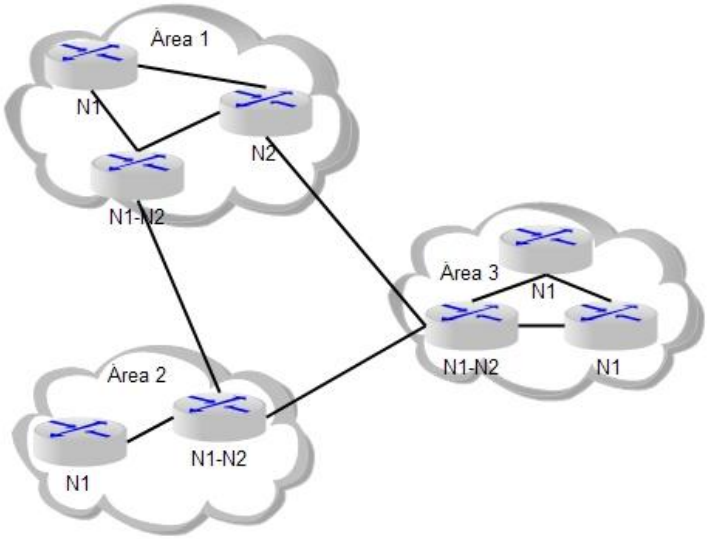

Fig. 2.13. Tres áreas dentro un AS utilizando el protocolo de IS-IS (Diagrama propio).

Los paquetes de estado de enlace IS-IS utilizan direcciones NSAP (Network Service Access Points, Servicio de Red de Punto de Acceso) para identificar el router y a la tabla de topología, las direcciones NSAP contienen un identificador del dispositivo llamado NET (Network Entity Title), estas direcciones tienen una longitud de 20 bytes como se muestra en la fig. 2.14.

Fig. 2.14. Campos de NSAP. [91]

IDP (Initial Domain Part): se encarga del enrutamiento externo entre AS.

DSP (Domain Specific Part): se encarga del enrutamiento dentro de un área.

AFI (Authority and Format Identifier): este campo tiene por defecto una longitud de 1 byte, especifica el formato de la dirección y quien la asigna.

IDI (Initial Domain Identifier): tiene una longitud de 2 bytes y especifica el número de área a la que pertenece el router

HODSP (High Order Domain Specific Part): es una subdireccion del dominio.

System ID: se encarga de identificar al dispositivo mediante su dirección MAC o mediante un valor

NSEL (NSAP selector): identifica a un usuario en la red el cual tiene un valor de 0 por lo que en IS-IS siempre se tendrá este valor. [91] [92]

El protocolo IS-IS forma dos tipos de adyacencias de ES-IS (End System to Intermediate System) y de IS-IS (Intermediate System to Intermediate System):

Adyacencia ES-IS: cuando se conectan los ES con los IS, los ES envían paquetes que permiten a un IS conocer qué ES se encuentran en la red y establecer una relación, los paquetes utilizados para establecer una relación entre ES-IS son los siguientes: paquetes ESH (End System Hello), son paquetes enviados por los dispositivos de una red hacia los routers para formar una relación. Paquetes ISH (Intermediate System Hello), son paquetes que envían los routers de una red para establecer relación con los ES.

Adyacencia IS-IS: es cuando forman relación dos o más IS dentro de un área, los paquetes utilizados para establecer una relación entre IS son:

- ✓ Nivel 1 IIH (IS IS Hello): utilizado para formar relación con dispositivos de nivel 1, estos utilizan una dirección MAC la cual indica que pertenecen a este nivel.
- ✓ Nivel 2 IIH: utilizado para formar una relación con dispositivos de nivel 2, los cuales utilizan una dirección MAC al igual que los de nivel 1 para indicar al nivel que pertenecen.
- ✓ Punto a punto IIH: son paquetes utilizados para crear relaciones con dispositivos que se encuentran conectados punto a punto y en el cual no existen niveles.

Tipos de paquetes IS-IS:

1. IIH (IS IS Hello): paquete utilizado para formar relaciones con sus vecinos.
2. LSP (Link State Packet): utilizado para intercambiar información del enrutamiento, los LSP tiene un identificador ID del sistema y existen dos tipos los de nivel 1 que sólo se propagan dentro de un área y los de nivel 2 que sólo se propagan por el enlace troncal.
3. NSP (Sequence Number Packet): utilizado para la sincronización de los LSDB (link State Data Base) y controla los LSP en su envió, existen dos tipos de NSP: los CSNP (Complete Sequense Number PDU (Unidad de Datos de Protocolo)) el cual contiene información de todas las LSP y los PSNP (Partial Secuence Number PDU) el cual contiene información de las LSDB.

IS-IS encapsula en la capa 2 del modelo OSI a diferencia de otros protocolos de enrutamiento que lo hacen en capa 3, como RIP, IGRP, EIGRP y OSPF. [92] [93]

Características:

1. Algoritmo de enrutamiento link state Dijkstra, el cual es utilizado por el algoritmo SPF (Shortest Path First).
2. La métrica utilizada es el costo (ancho de banda).
3. Utiliza una arquitectura jerárquica esta tiene prioridad sobre una topología creada a través de direccionamiento.
4. Pertenece a los protocolos con clase, soporta VLSM.
5. Cuenta con autentificación.

A manera de resumen en la tabla 2.3 se muestra la comparación de los distintos protocolos de enrutamiento IGP que se han abordado.

Protocolo de ruteo	**RIP**	**RIP v2**	**IGRP**	**EIGRP**	**OSPF**	**IS-IS**
Algoritmo de enrutamiento	BELLMAN-FORD	BELLMAN-FORD	BELLMAN-FORD	DUAL	DIJKSTRA	DIJKSTRA
	Distance Vector	Distance Vector	Distance Vector		Link State	Link State
Tipo de protocolo	IGP	IGP	IGP	IGP	IGP	IGP
Métrica	Saltos	Saltos	compuesta	compuesta	Ancho de banda	Ancho de banda
Soporta VLSM		✓		✓	✓	✓
Topología jerárquica					✓	✓
Equilibrio de la carga-iguales	✓	✓	✓	✓	✓	✓
Equilibrio de la carga-desiguales		✓	✓	✓		
Convergencia	Lento	Lento	Lento	Rápido	Rápido	Rápido
Escalabilidad	Pequeña	Pequeña	Mediana	Grande	Grande	Muy grande

Tabla 2.3 Comparación de los protocolos de enrutamiento. [81] [82]

Capítulo 3

Simulación del Backbone de la Red Avanzada I2 en México

3.1 Introducción

En este capítulo se presentan los resultados de la simulación hecha con Packet Tracer V5.3 de CISCO, las características del equipo en que se realizó la simulación son: Laptop HP Pavilion g4, Procesador Intel(R) Core(TM) i3-2330M, CPU @ 2.20Ghz, RAM 4GB, Sistema operativo Windows 7 Home Basic, Service Pack 1, (Sistema Operativo de 64 bits).

Para realizar la simulación se eligió una red de “clase B” ya que con esta se pueden formar 16,384 redes con 65,534 equipos cada una, en caso de que se requiera expandir la red en un futuro, la red a utilizar es la 172.2.X.X. El protocolo de gateway interior empleado fue OSPF para la configuración de cada router.

Para realizar las pruebas de comunicación y como una medida para diagnosticar la conectividad entre cada uno de los dispositivos con los que cuenta el backbone de la red I2 de México se utilizará el proceso ping, este a su vez empleará los protocolos ARP definido en el RFC 826 e ICMP definido en el RFC 792. [94] [95]

El objetivo de simular la red CUDI es conocer cómo está constituida toda su infraestructura de telecomunicaciones y verificar qué tan viable es simular la red por medio de Packet Tracer de CISCO V5.3.

3.2 Simulación Packet tracer v5.3

En la simulación se empleó la topología de la red CUDI de la fig. 3.1, la cual es parcial ya que sólo cuenta con el Backbone y con 8 asociados, esto debido a las características del equipo en que se realizara la simulación.

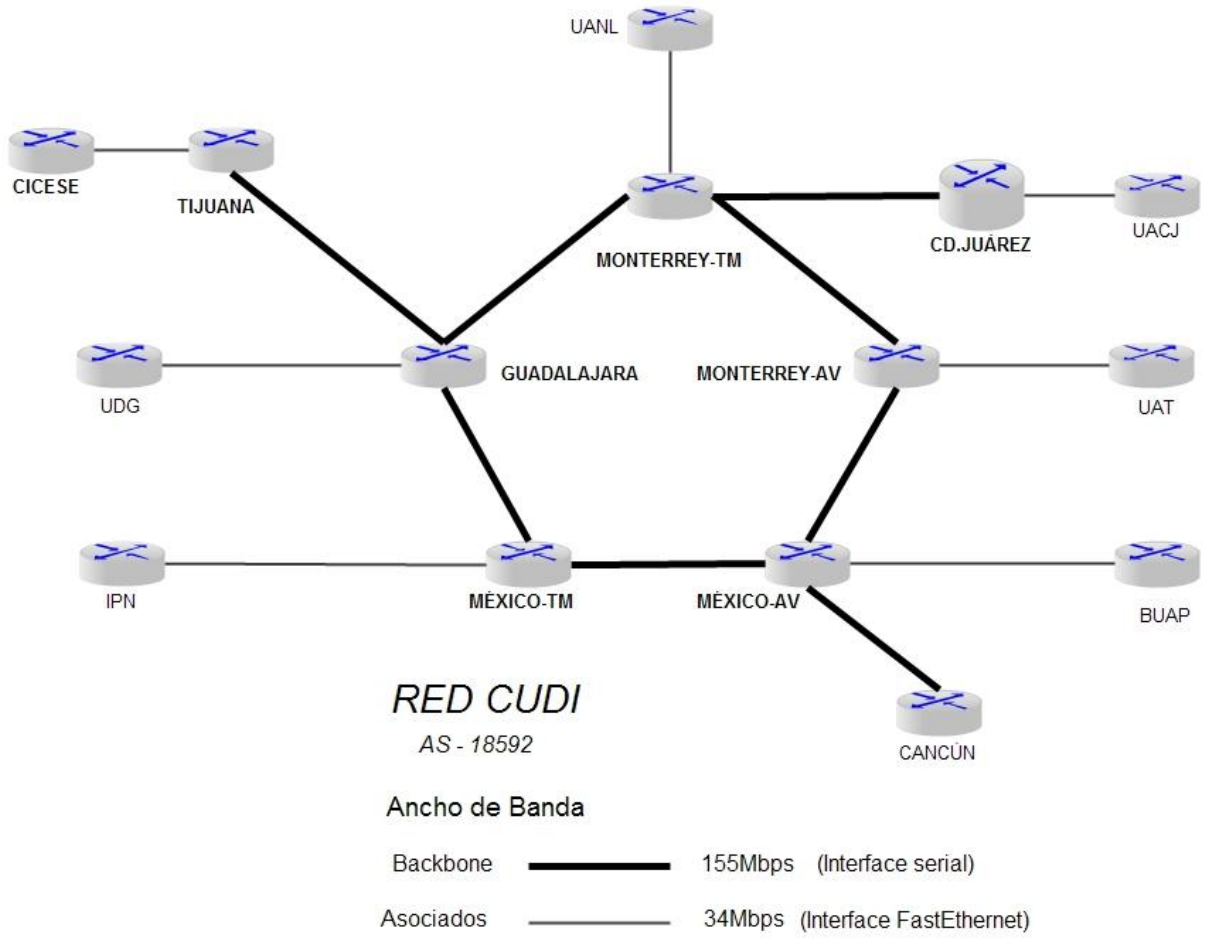

Fig. 3.1 Topología de Backbone de CUDI, 2013 (Diagrama propio).

Para la simulación se emplearon direcciones IP de clase B, las cuales empiezan con 128.0.X.X y terminan en 191.255.X.X, con esta clase de direcciones IP se pueden formar 16,384 redes con 65,534 equipos. Para cada una de las interfaces de los routers de la red CUDI se utilizaron las direcciones indicadas en la tabla 3.1, mientras que para realizar el enrutamiento se utilizaron las direcciones IP como se muestran en la tabla 3.2.

Por su parte los host utilizaron las direcciones IP que se encuentran en la tabla 3.3 para que cada uno de los host se comuniquen entre ellos. [Apéndice B]

Router	Dirección IP					Mascara de red
	S 1/0	S 1/1	S 1/2	S 1/3	Fa 0/0	/16
México-TM	172.2.1.1	172.6.1.2	172.7.1.2			✓
IPN	172.7.1.1				172.18.1.1	✓
						✓
México-AXT	172.2.1.2	172.3.1.1	172.16.1.1	172.15.1.1		✓
BUAP	172.15.1.2				172.24.1.1	✓
Cancún	172.16.1.2	172.17.1.1				✓
UQROO	172.17.1.2				172.25.1.1	✓
						✓
Monterrey-TM	172.4.1.2	172.5.1.1	172.12.1.1	172.11.1.2		✓
UANL	172.11.1.1				172.21.1.1	✓
CD-Juárez	172.12.1.2	172.13.1.1				✓
UACJ	172.13.1.2				172.22.1.1	✓
						✓
Monterrey-AXT	172.3.1.2	172.4.1.1	172.14.1.1			✓
UAT	172.14.1.2				172.23.1.1	✓
						✓
Guadalajara-TM	172.5.1.2	172.6.1.1	172.9.1.2	172.8.1.2		✓
UDG	172.8.1.1				172.19.1.1	✓
Tijuana	172.9.1.1	172.10.1.2				✓
CICESE	172.10.1.1				172.20.1.1	✓

Tabla 3.1 Direcciones IP utilizadas para cada uno de las interfaces de los routers de la Red CUDI

Direcciones de red para configurar cada router por medio de OSPF.

Router	Direcciones de Red	Mascara de red
		/16
México-TM	172.2.0.0, 172.6.0.0, 172.7.0.0	✓
IPN	172.7.0.0, 172.18.0.0	✓
		✓
México-AXT	172.3.0.0, 172.2.0.0, 172.16.0.0, 172.15.0.0	✓
BUAP	172.15.0.0, 172.24.0.0	✓
Cancún	172.16.0.0, 172.17.0.0	✓
UQROO	172.17.0.0, 172.25.0.0	✓
		✓
Monterrey-TM	172.5.0.0, 172.4.0.0, 172.12.0.0, 172.11.0.0	✓
UANL	172.11.0.0, 172.21.0.0	✓
CD-Juárez	172.12.0.0, 172.13.0.0	✓
UACJ	172.13.0.0, 172.22.0.0	✓
		✓
Monterrey-AXT	172.4.0.0, 172.3.0.0, 172.14.0.0	✓
UAT	172.14.0.0, 172.23.0.0	✓
		✓
Guadalajara-TM	172.5.0.0, 172.6.0.0, 172.9.0.0, 172.8.0.0	✓
UDG	172.8.0.0, 172.19.0.0	✓
Tijuana	172.9.0.0, 172.10.0.0	✓
CICESE	172.10.0.0, 172.20.0.0	✓

Tabla 3.2 Direcciones IP utilizadas para el enrutamiento de los routers de la Red CUDI, utilizando OSPF

La red CUDI incluye un host por asociado a los cuales se enviaron ping, estos cuentan con las direcciones IP de la tabla 3.3.

HOST	Dirección IP	Gateway
IPN	172.18.1.2 /16	172.18.1.1
UDG	172.19.1.2 /16	172.19.1.1
CICESE	172.20.1.2 /16	172.20.1.1
UANL	172.21.1.2 /16	172.21.1.1
UACJ	172.22.1.2 /16	172.22.1.1
UAT	172.23.1.2 /16	172.23.1.1
BUAP	172.24.1.2 /16	172.24.1.1
UAQROO	172.25.1.2 /16	172.25.1.1

Tabla 3.3 Direcciones IP utilizados por los host de la Red CUDI

Para realizar la simulación en Packet Tracer de la Red CUDI, como se muestra en la fig. 3.1, se emplearon los siguientes equipos: host, routers 2811 con versión de IOS 12.4 y switches WS-C2960-24TT con versión del IOS 12.2, ya que este simulador no cuenta con los equipos core que emplea la red CUDI como el router 7200 y el switch SW-BPX 8600. Dentro del simulador de Packet Tracer se colocan los equipos utilizados para crear la red CUDI de manera aproximada, como se ve en la fig. 3.2.

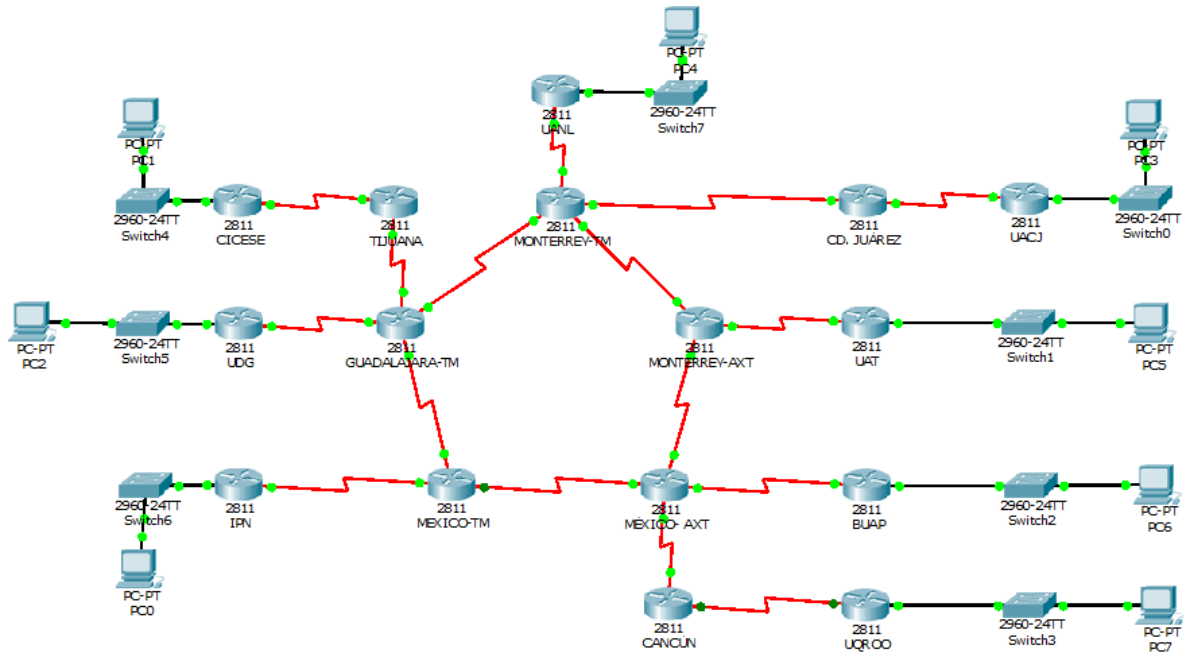

Fig. 3.2 Topología de Backbone de CUDI, creada en el simulador Packet Tracer V5.3.

Una vez realizada nuestra red CUDI en el simulador se procede a configurar cada uno de nuestros dispositivos con los que cuenta la red, empleando las direcciones IP de las tablas 3.1, 3.2 y 3.3.

En los routers se deben configurar sus interfaces así como el protocolo de enrutamiento a utilizar, en este caso se utilizó el IGP-OSPF, el cual es empleado por la red CUDI.

3.3 Configuración de Router y Host

La configuración de cada uno de los routers con los que cuenta la red CUDI se configuraron por medio de CLI (Command Line Interface, Interfaz de Línea de Comandos) del IOS (Internetworking Operating System, Sistema Operativo de Interconexión de Redes) de Cisco, parecido como se haría desde la consola de un equipo real, todos los router se configuraron con los mismos comandos, sólo cambiaron las direcciones IP utilizadas por los routers y sus interfaces. La fig. 3.3 muestra la configuración para el router CICESE. [Apéndice D]

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CICESE
CICESE(config)#interface serial 1/0
CICESE(config-if)#ip address 172.10.1.1 255.255.0.0
CICESE(config-if)#clock rate 56000
CICESE(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial1/0, changed state to down
CICESE(config-if)#exit
CICESE(config)#router ospf 1
CICESE(config-router)#network 172.10.0.0 0.0.255.255 area 0
CICESE(config-router)#exit
CICESE(config)#
```

Fig. 3.3 Configuración del router CICESE por medio de CLI de CISCO.

Enseguida se configuraron los host con las direcciones IP de la tabla 3.3 para cada uno de los host de la red CUDI, en la fig. 3.4 se muestra un ejemplo de la

configuración del host CICESE a la cual se le configura la dirección IP, la máscara de subred y el Gateway.

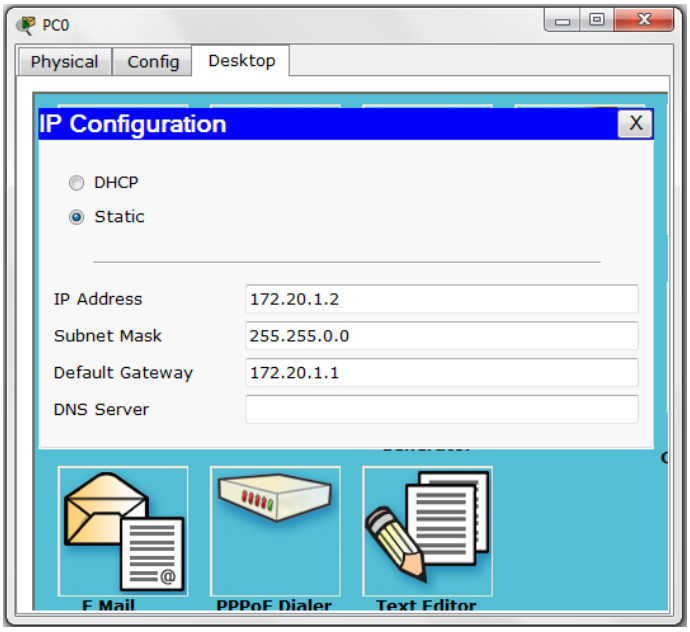

Fig. 3.4 Configuración del host CICESE.

3.4 Simulación

Una vez realizada la configuración de cada uno de los equipos de la red CUDI se procedió a realizar la simulación enviando PING (Packet Internet Groper, Buscador de Paquetes en Redes), este es una herramienta de diagnóstico para verificar la conexión entre hosts de una red. Para nuestro ejemplo, se envió un ping del host1 que se encuentra en el CICESE hacia el host7 que se encuentra en UQROO. Para realizar la simulación se utilizó el *"modo simulación"* en el área de trabajo para poder visualizar el envió de paquetes del host1 al host7, lo que permitió hacer un análisis detallado del tráfico en la red, en este modo seleccionamos los protocolos ICMP y ARP los cuales son utilizados por el proceso ping, en la fig. 3.5 se muestran los paquetes ICMP y ARP los cuales se encuentran en el host1.

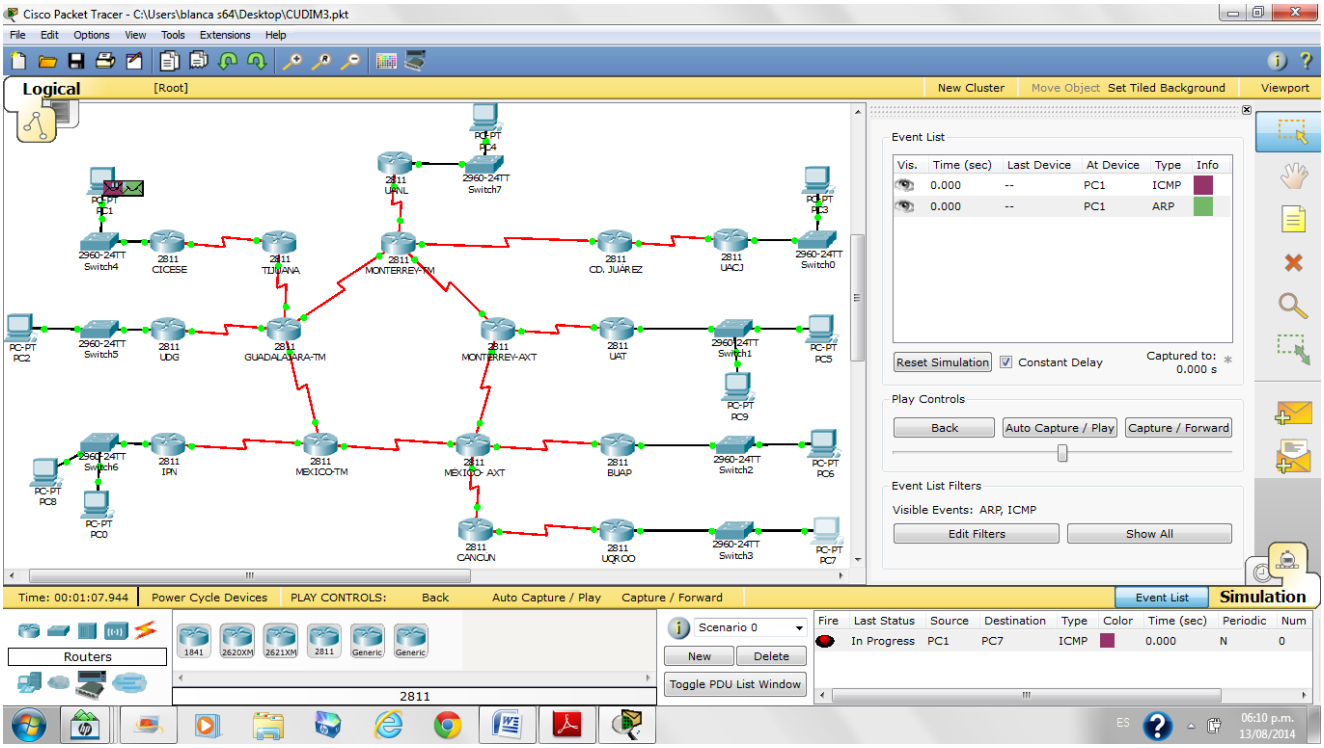

Fig. 3.5 Área de trabajo de Packet Tracer, en modo simulación.

Al enviar un ping del host1 al host7 para que se comuniquen entre ellas, se llevó a cabo el proceso ping el cual comienza en la capa 5 del modelo TCP/IP, posteriormente se manda llamar al proceso ICMP el cual se encuentra en la capa 3 del modelo TCP/IP el cual se apoya en el protocolo ICMP para la construcción de paquetes.

Como ICMP no cuenta con la dirección MAC destino se recurre al proceso ARP para completar la tabla ARP el cual se encuentra en capa 2, el proceso ARP construye un paquete ARP por medio del protocolo ARP el cual manda un mensaje echo request ARP, ver fig. 3.6.

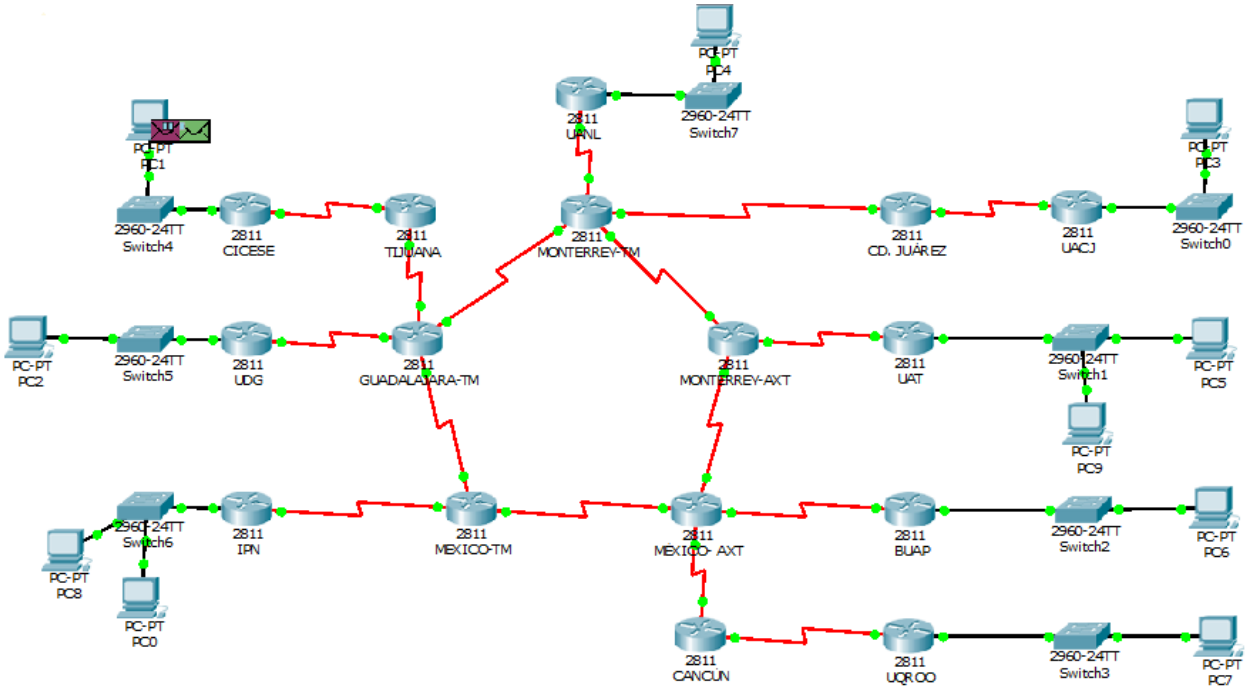

Fig. 3.6 El proceso ping se apoya en el proceso ICMP y el proceso ARP.

La fig. 3.7 muestra el frame IP, el paquete ICMP en el cual se observa la dirección destino y la dirección origen, se observa también el Frame de Ethernet II y el paquete ARP, en el que se observa que hace falta la dirección MAC destino.

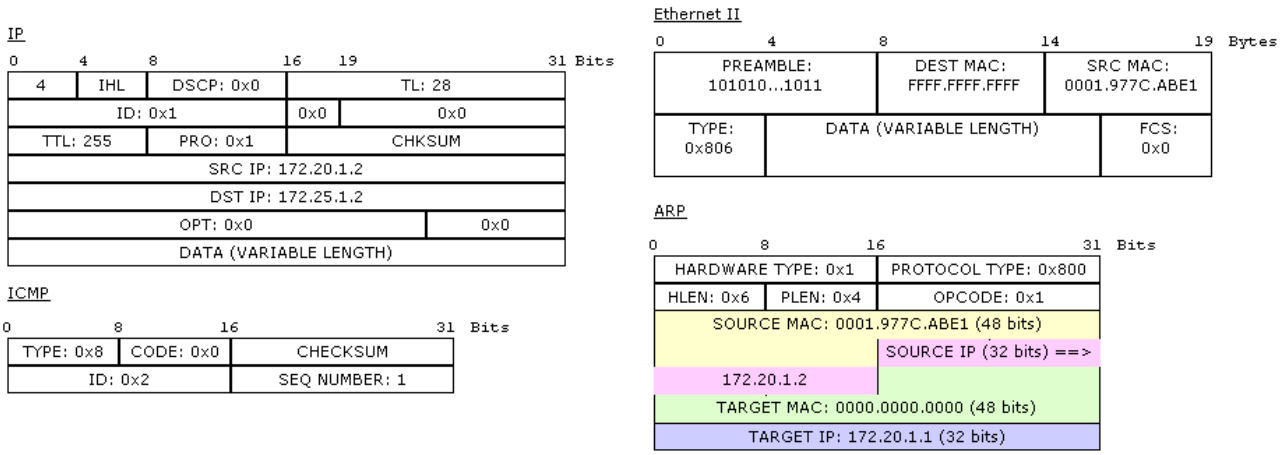

Fig. 3.7 Frame IP, Ethernet y paquetes ICMP, ARP.

El paquete ARP se encapsula dentro de un frame Ethernet II, el cual pasa a capa 1 y posteriormente al switch 4 aquel que se encuentra conectado al router CICESE. El paquete sube a capa dos y baja a capa uno dentro del switch 4 el cual manda el paquete a todos los puertos de los host menos al que lo envió, como se ve en la fig. 3.8.

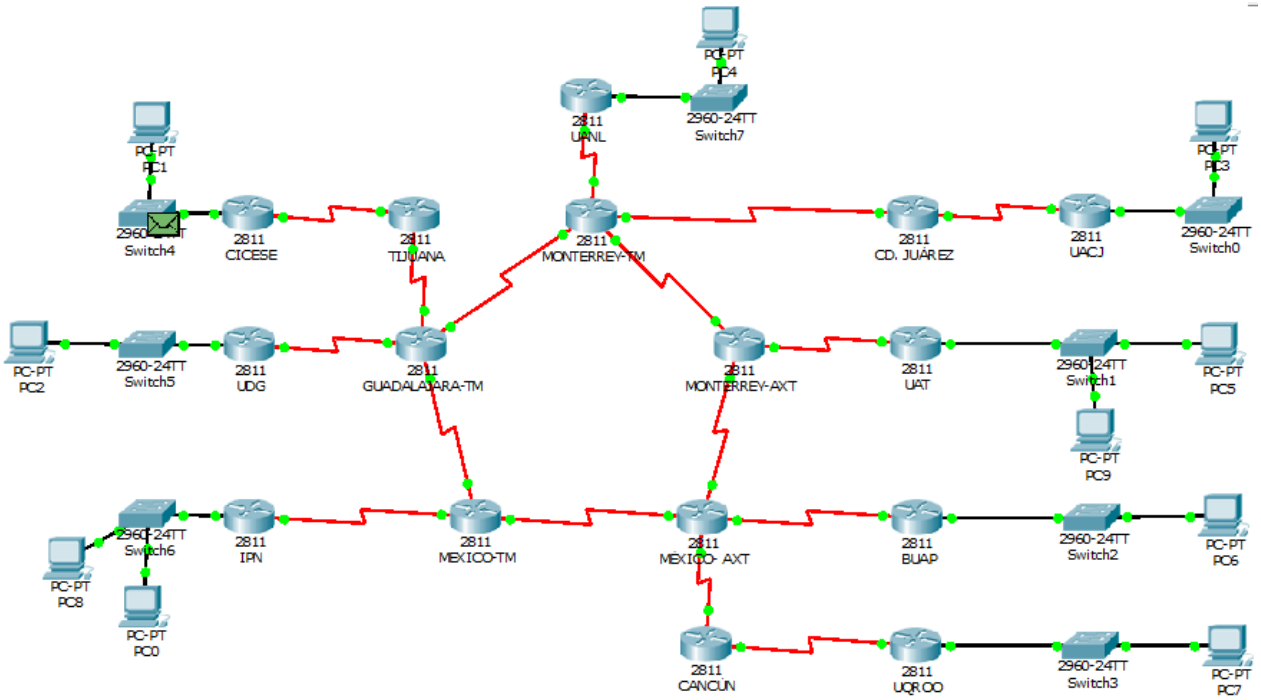

Fig. 3.8 El frame request ARP llega al switch 4.

Posteriormente el paquete es recibido pero los paquetes son desechados (por lo que realiza un Drop) por las NIC de los demás host para quienes no era el paquete, esto ocurre al tener más host conectados al switch 4, en este caso la NIC que recibió el paquete fue el del router CICESE para quien estaba dirigida la trama Ethernet II, este lo desencapsula en capa 2, actualiza su tabla ARP y responde con un mensaje echo replay ARP. El router no puede enviar paquetes broadcast, como se muestra en la fig. 3.9.

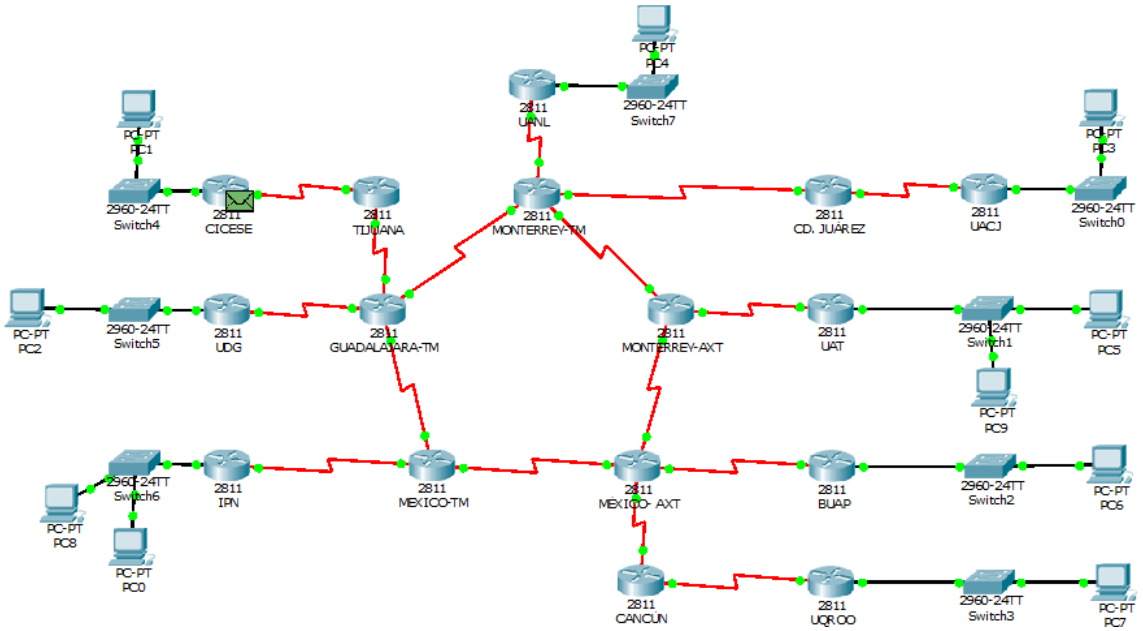

Fig. 3.9 El frame request ARP llega al router CICESE.

En la fig. 3.10 se muestra como el campo de la dirección MAC destino cambió de FFFF.FFFF.FFFF a 0001.977C.ABE1 y la dirección MAC fuente cambió por 00D0.FF5B.0901 esta dirección MAC corresponde a la NIC del router CICESE.

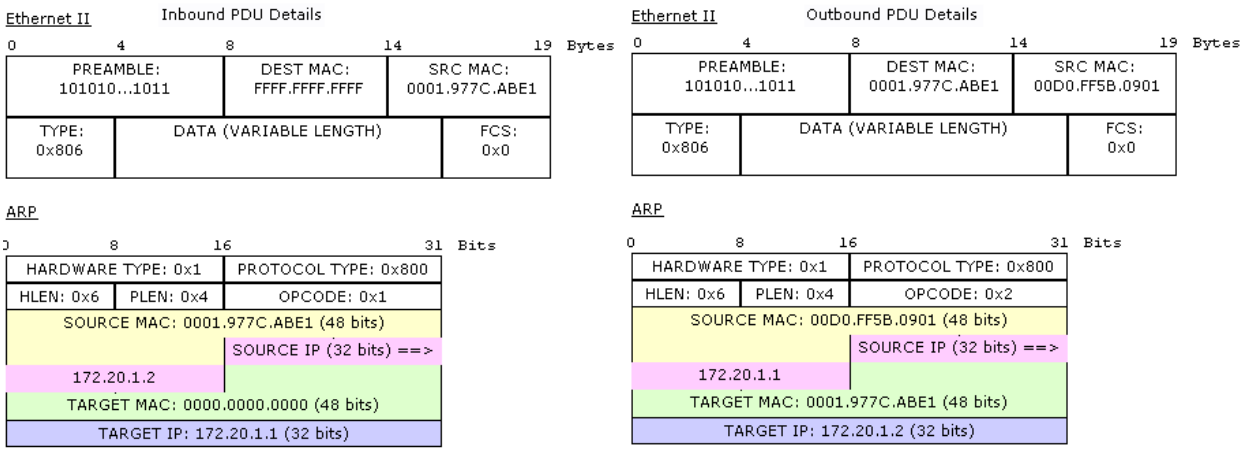

Fig. 3.10 Campo de la MAC destino cambia.

El mensaje echo replay ARP generado por el router CICESE es enviado hacia el switch 4, el switch 4 envía el frame sólo al puerto que tiene conectado el host1, fig. 3.11.

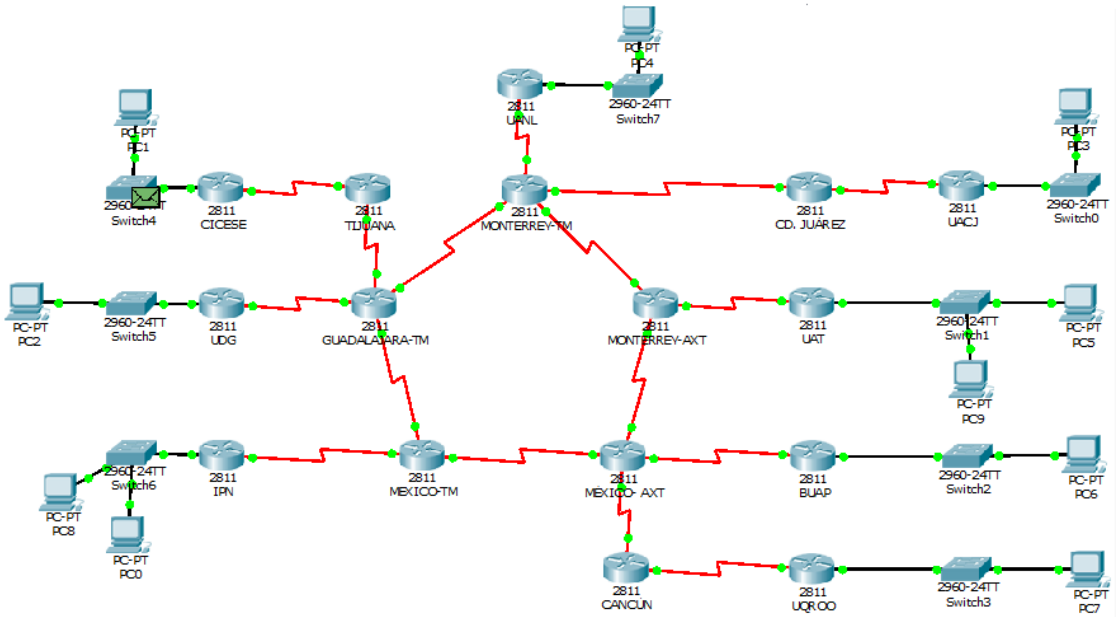

Fig. 3.11 El router CICESE envía un frame replay ARP hacia el switch 4.

El host1 recibe, desencapsula, e identifica el mensaje replay ARP, llegando el frame replay ARP con éxito al host1 como se muestra en la fig. 3.12, con lo cual finaliza el proceso ARP. Una vez que se actualizó la tabla ARP del host1, el proceso ICMP permite encapsular al mensaje request ICMP el cual se encontraba en el buffer el cual se envía hacia el switch 4, una vez que el switch 4 recibe el paquete request ICMP lo envía hacia el router CICESE.

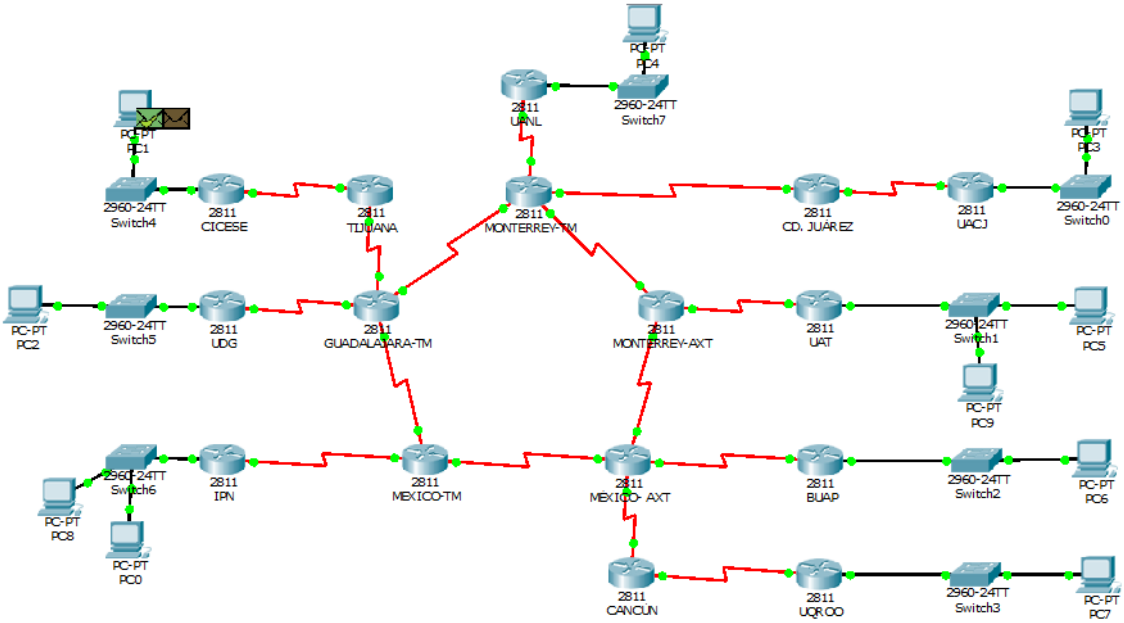

Fig. 3.12 El frame replay ARP llega con éxito a la PC1.

En la fig.3.13 se muestra la entrada del paquete ARP y la salida del mensaje request ICMP el cual es encapsulado en la trama Ethernet.

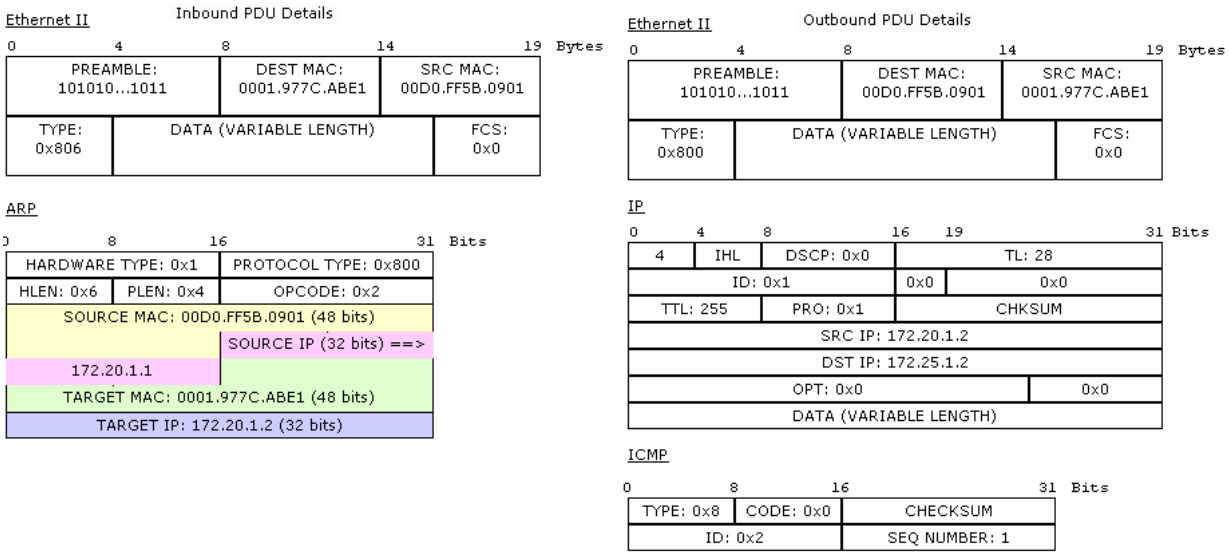

Fig. 3.13 EL frame Ethernet es completado con la dirección MAC de la NIC del router CICESE.

El switch 4 recibe el paquete request ICMP y lo envía al router CICESE sólo por el puerto al que se encuentra conectado el router, el paquete recibido es un paquete unicast, como se muestra en la fig.3.14.

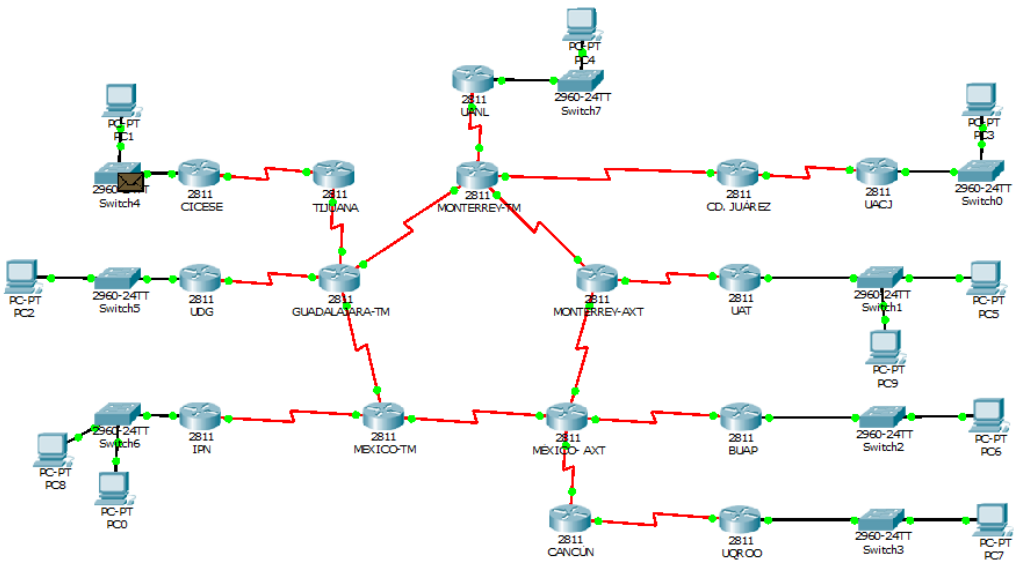

Fig. 3.14 Switch 4 recibiendo el paquete request ICMP enviado por el host1.

Una vez que el paquete request ICMP llega al router CICESE fig. 3.15, el router busca en su tabla de direcciones ARP la dirección destino, pero éste encuentra una dirección de red en su tabla de enrutamiento a través de la cual se puede alcanzar la red destino, esta red destino se puede alcanzar a través de la dirección 172.10.1.2, por lo que el router CICESE envía el paquete request ICMP al router Tijuana el cual cuenta con esta dirección.

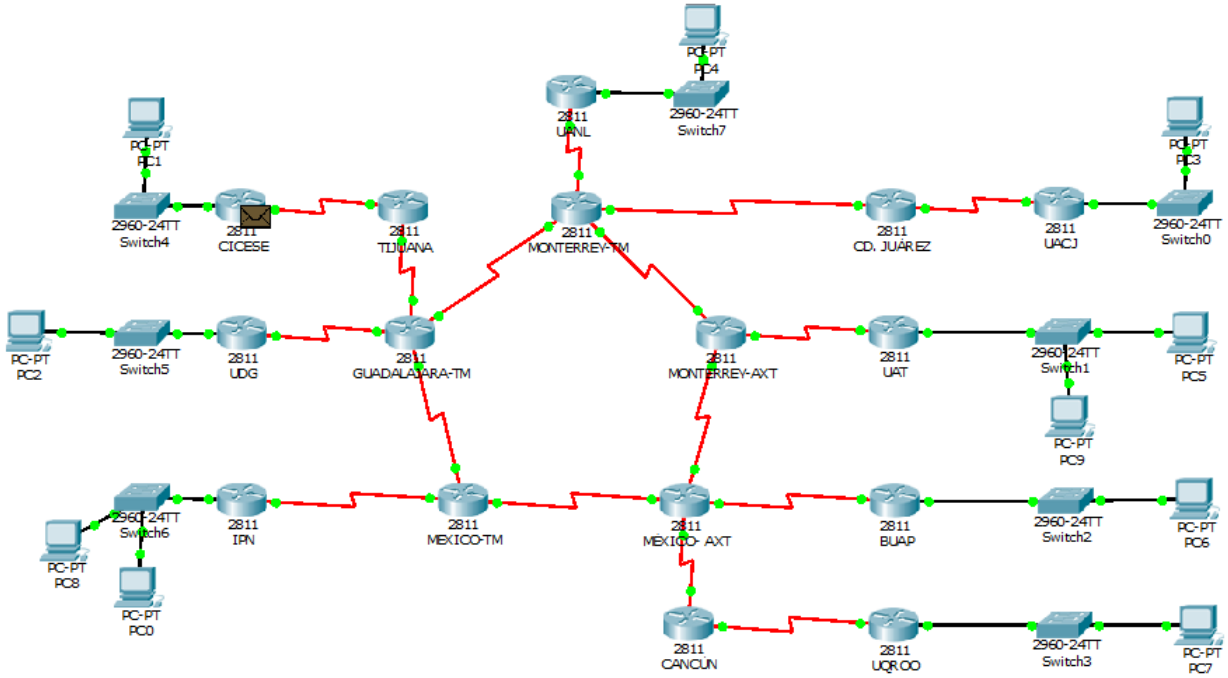

Fig. 3.15 Paquete request ICMP recibido por el router CICESE.

El router Tijuana envía el paquete request ICMP a través de la dirección 172.9.1.2 hacia el router Guadalajara, ver la fig. 3.16.

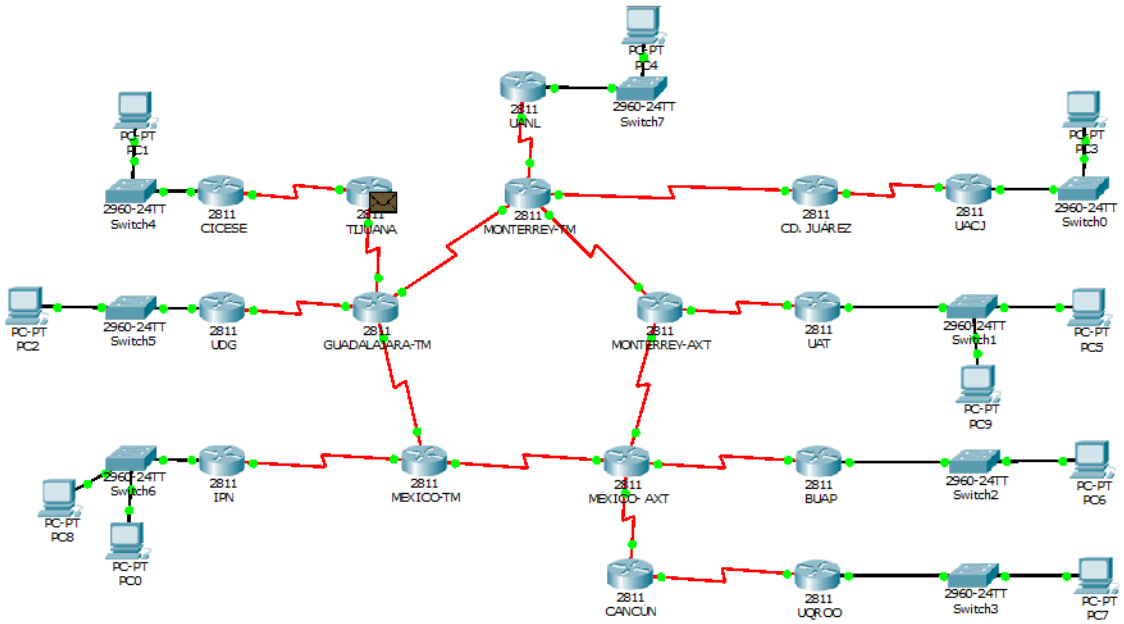

Fig. 3.16 Paquete request ICMP recibido por el router Tijuana.

El router Guadalajara envía el paquete request ICMP a través de la dirección 172.6.1.2 hacia el router México, como se muestra en la fig. 3.17.

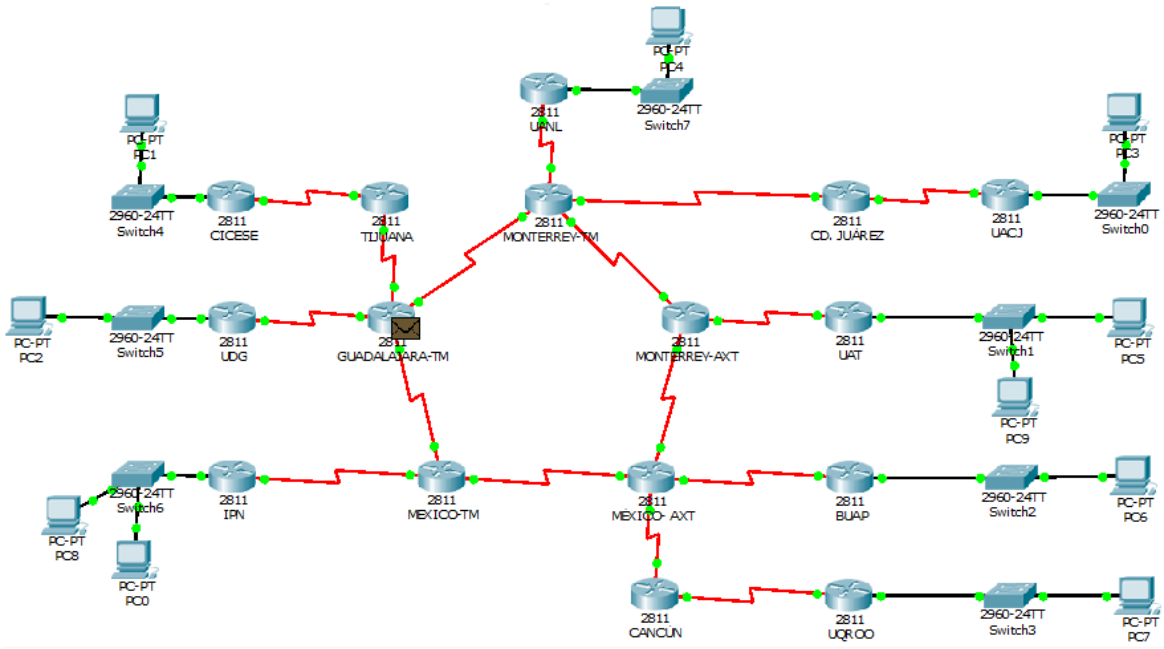

Fig. 3.17 Paquete request ICMP recibido por el router Guadalajara-TM.

El router México TM envía el paquete request ICMP a través de la dirección 172.2.1.2 hacia el router México AXT, como se muestra en la fig. 3.18.

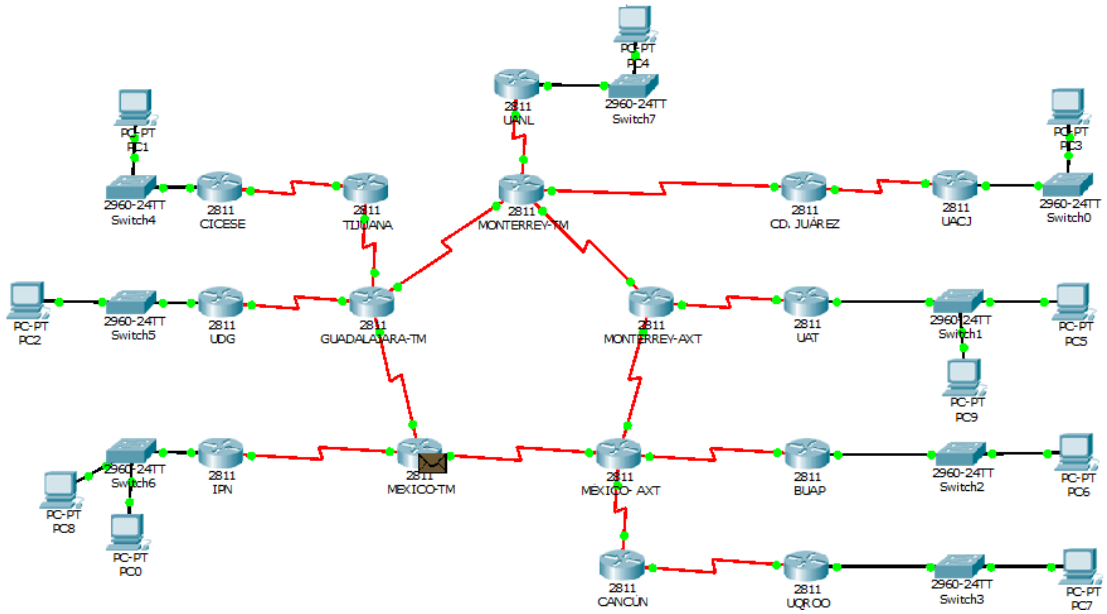

Fig. 3.18 Paquete request ICMP recibido por el router México-TM.

El router México AXT recibe el paquete request ICMP como se muestra en la fig. 3.19, y se envía el paquete request ICMP a través de la dirección 172.16.1.2 hacia el router Cancún.

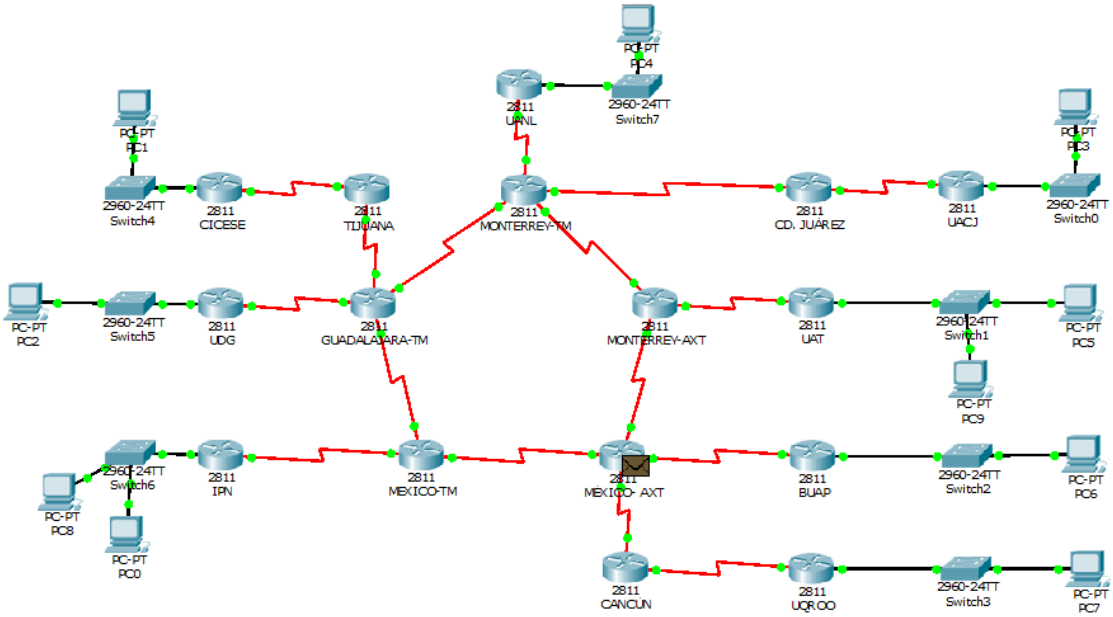

Fig. 3.19 Paquete request ICMP recibido por el router México-AXT.

El router Cancún envía el paquete request ICMP a través de la dirección 172.17.1.2 hacia el router UQROO, como se indica en la fig. 3.20.

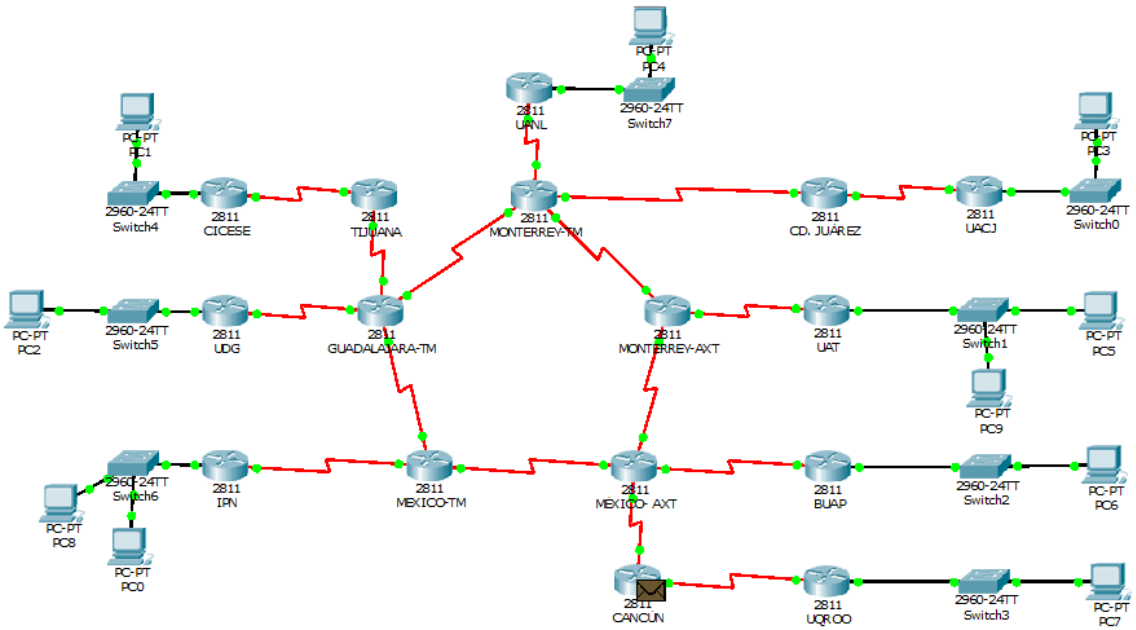

Fig. 3.20 Paquete request ICMP recibido por el router Cancún.

El router UQROO encuentra en su tabla de enrutamiento la dirección destino, como el router no contiene la dirección IP destino en su tabla ARP, el router envía un frame request ARP para completar el paquete ICMP, como se muestra en la fig. 3.21.

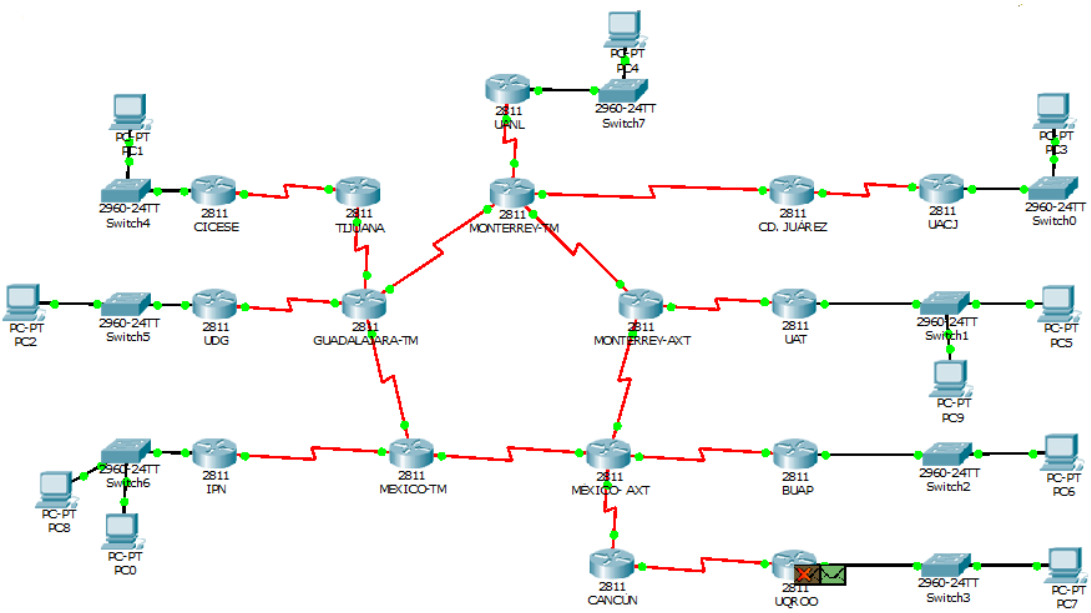

Fig. 3.21 Paquete request ICMP recibido por el router UQROO y construcción del frame request ARP.

En la fig. 3.22 se muestran las tramas IP, del paquete request ICMP que llegaron al router UQROO y la trama de Ethernet II junto con la trama request ARP que se utilizará para llegar al host 7.

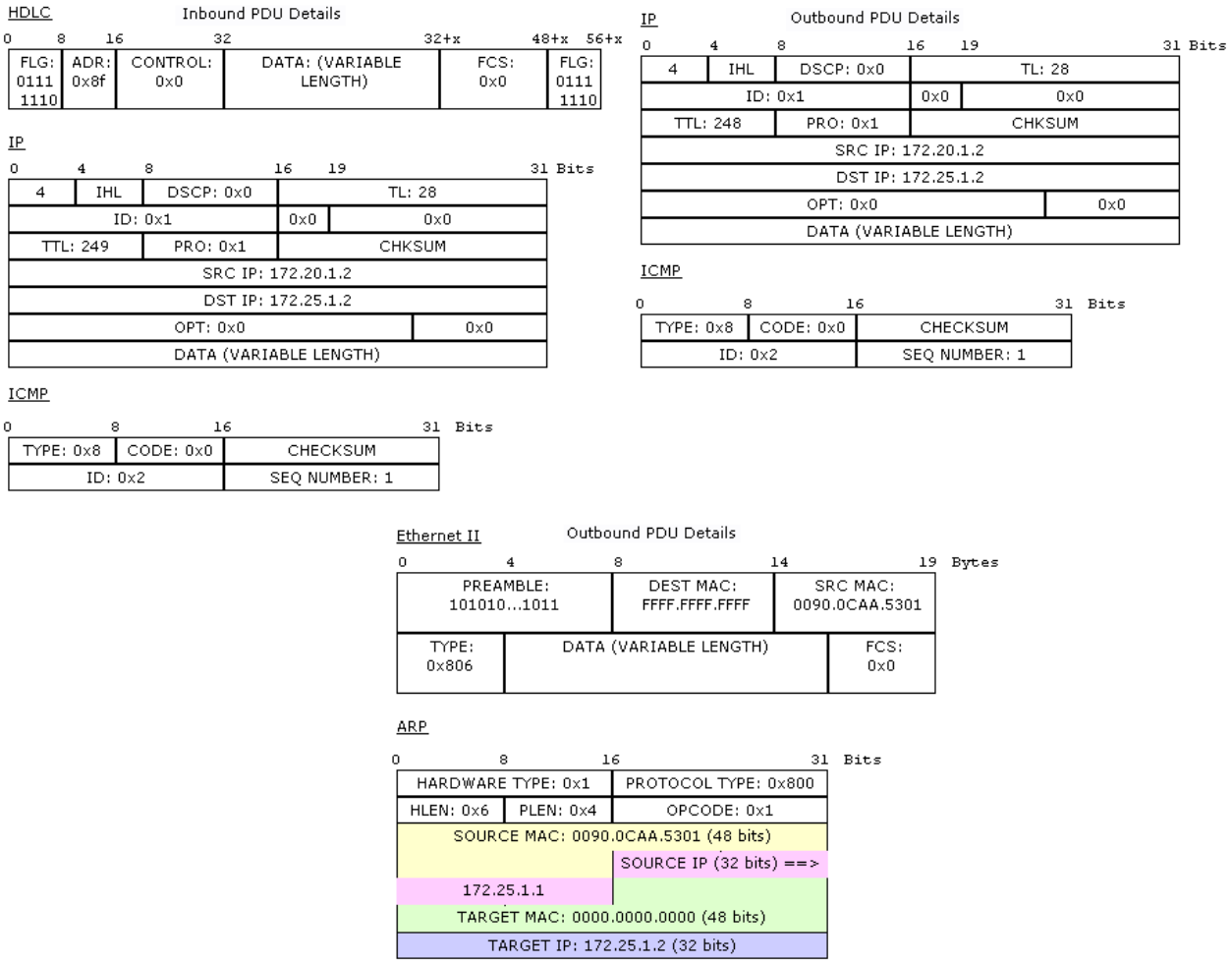

Fig. 3.22 Paquete request ICMP y construcción del frame request ARP en el router UQROO.

El frame request ARP es enviado al switch 3 como se muestra en la fig. 3.23, el cual realiza un broadcast hacia todos sus puertos excepto por el puerto que recibió el frame request ARP.

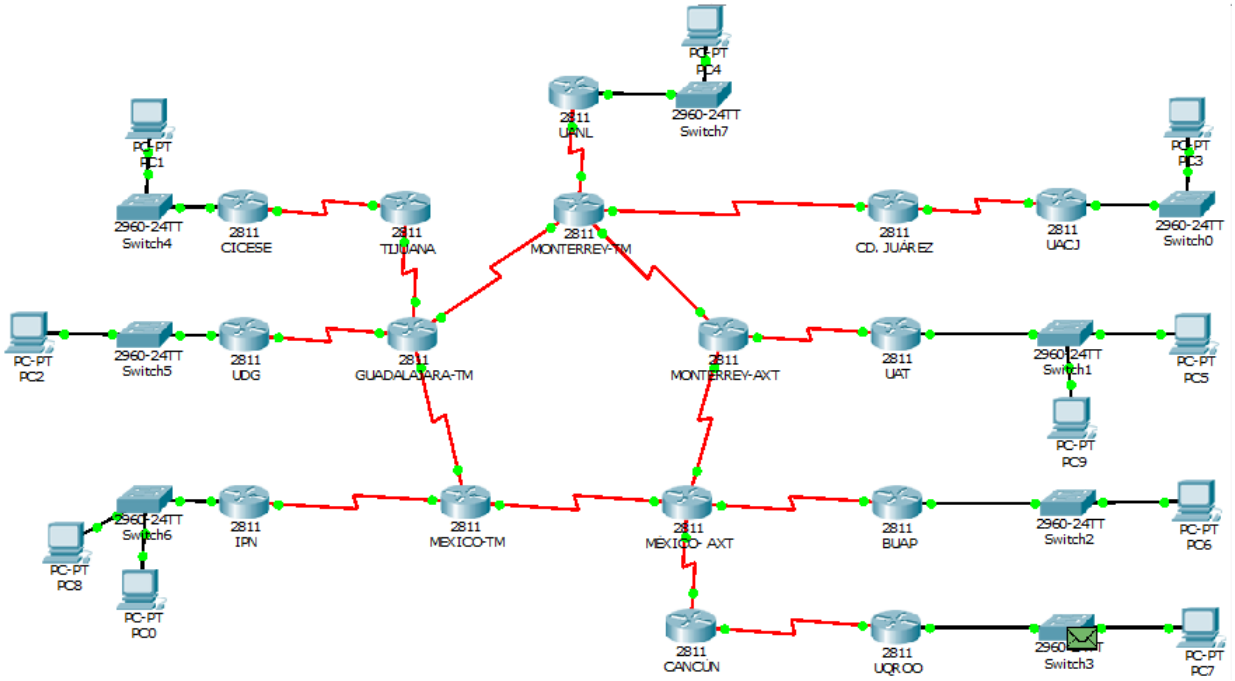

Fig. 3.23 Router UQROO enviando el frame request ARP al SW3.

El host7 reenvía un frame replay ARP hacia el router UQROO, antes de llegar al router UQROO el frame replay ARP pasa por el switch, éste sólo envía el frame al puerto que está conectado el router UQROO.

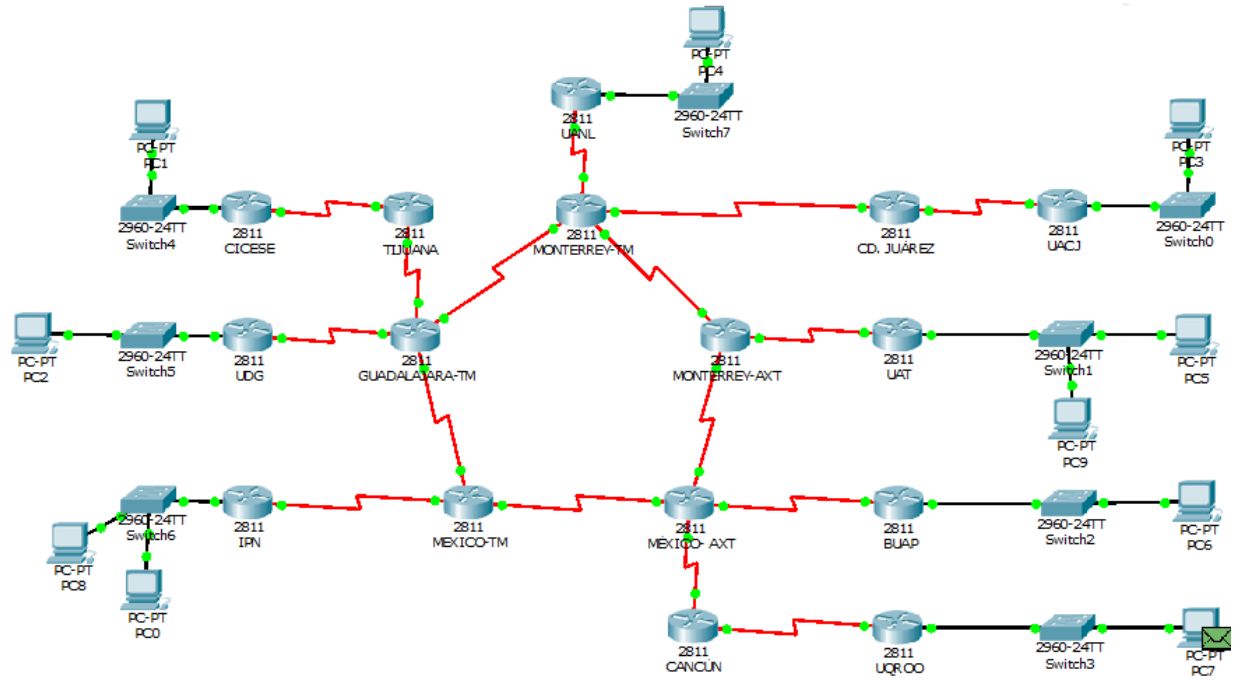

Fig. 3.24 Frame request ARP recibido por el host7.

Como se muestra en la fig. 3.25 los campos de la dirección MAC fuente y destino se cargan en la trama Ethernet.

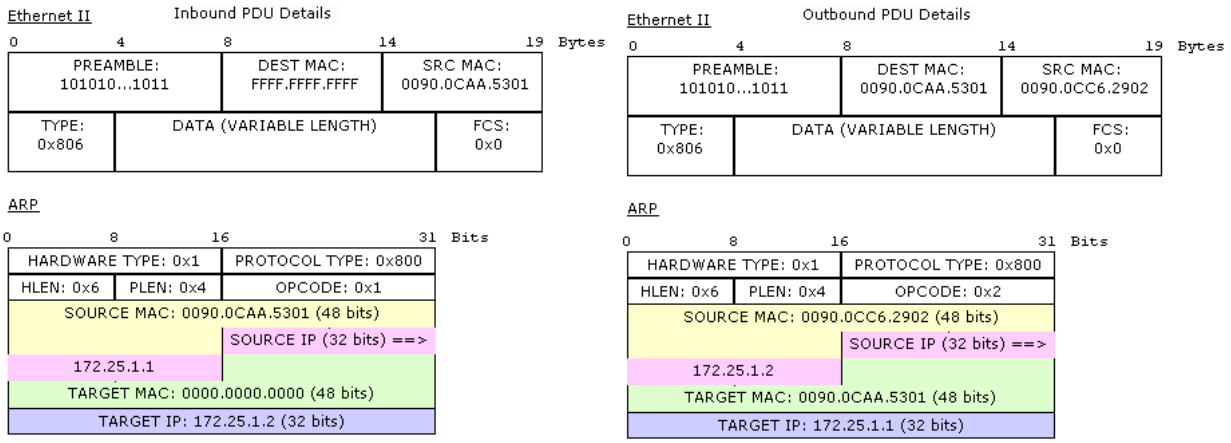

Fig. 3.25 El host7 envía un frame replay ARP al switch 3.

El router UQROO recibe con éxito el frame replay ARP como se muestra en la fig. 3.26, el router actualiza su tabla ARP y queda conformado el paquete ICMP.

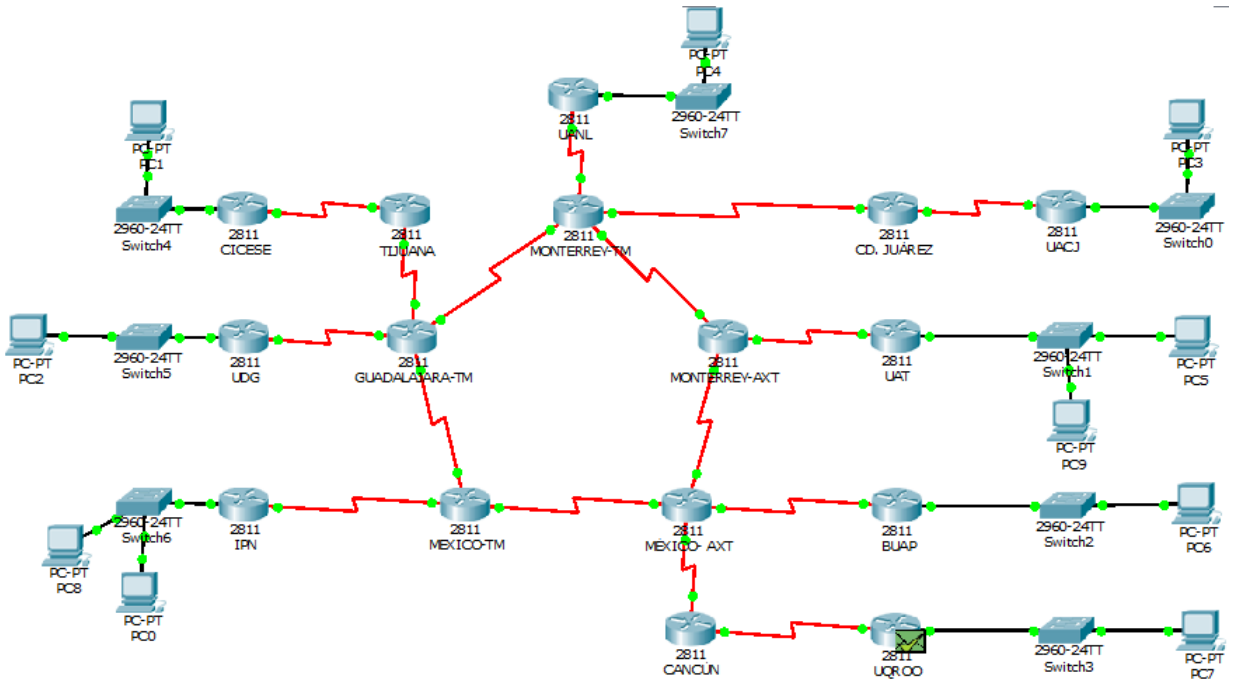

Fig. 3.26 El router UQROO recibe con éxito el frame replay ARP.

En este punto de la simulación el buffer del simulador se llenó y debe de limpiarse la lista de eventos del simulador como se muestra en la fig. 3.27. Esto muestra algunas limitaciones del simulador Packet Tracer.

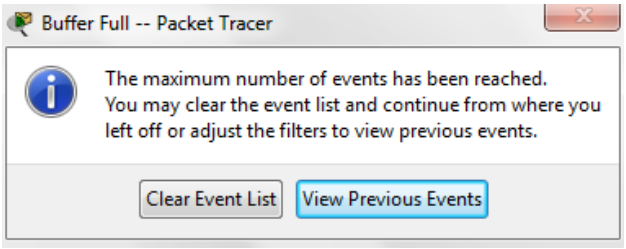

Fig. 3.27 El buffer del simulador es llenado.

El paquete ICMP es completado en el router UQROO este paquete es nuevamente enviado hacia el host1 siguiendo el camino: router CANCUN - router México AXT - router México TM - router Guadalajara – router Tijuana – router CICESE. El paquete ICMP llega finalmente a la NIC del host1 en donde el paquete ICMP se desencapsula con éxito y el proceso ping termina, una vez realizado el ping del host1 y el host7 se pueden comunicar entre ellos. El camino antes descrito no se puede visualizar en el simulador debido a que el buffer del simulador se llenó. Una vez limpiado el buffer, enviamos nuevamente un ping entre el host1 y el host7, el host1 sólo manda paquetes ICMP ya que conoce la dirección IP y la MAC del host destino, en la fig. 3.28 se muestran las tramas enviadas por el host1 y las recibidas por el host7.

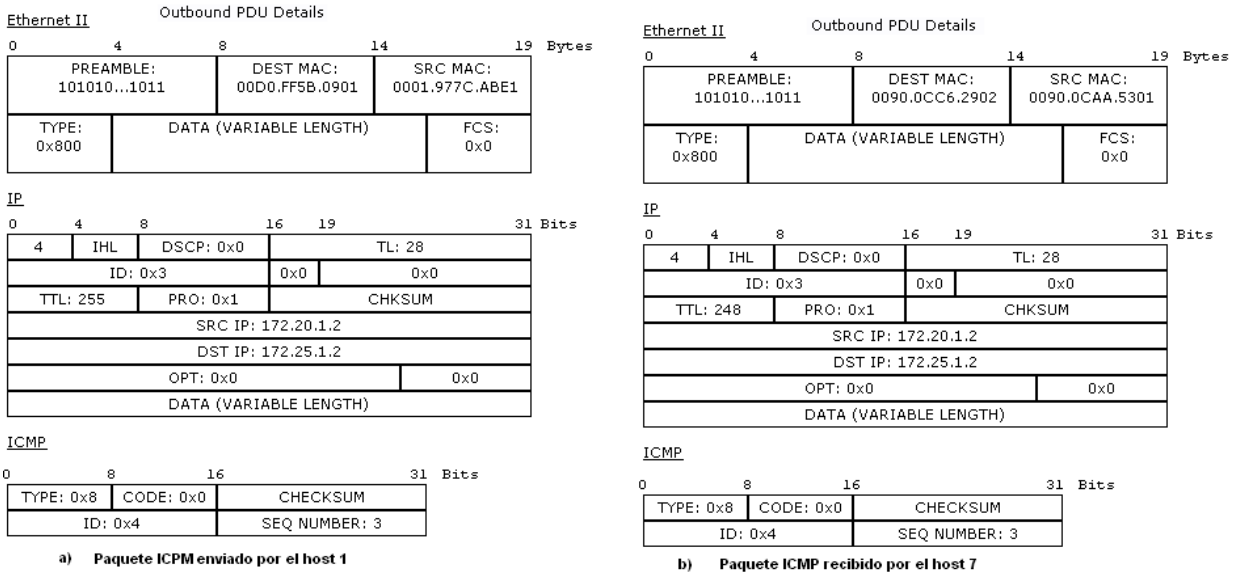

Fig. 3.28 a) Tramas que se envían desde el host1, b) tramas que son recibidas por el host7.

La fig. 3.29 muestra el paquete ICMP que se envió hacia la host7 desde el host1.

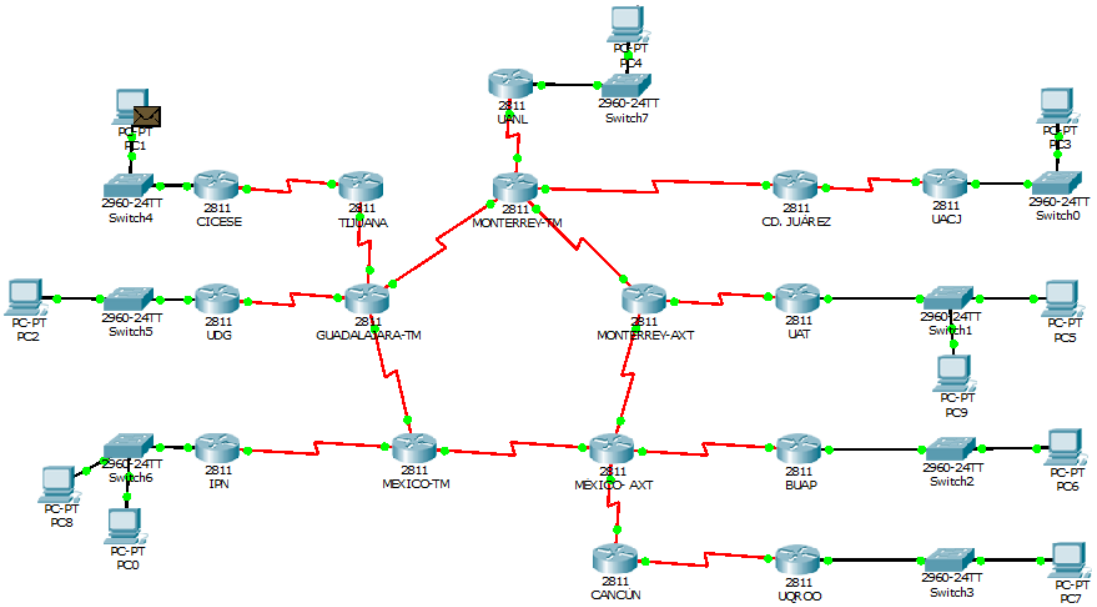

Fig. 3.29 Paquete ICMP listo para ser enviado a la PC7.

Una vez que el paquete request ICMP llega a la PC7 ésta envía un paquete replay ICMP hacia la PC1, como se muestra en la fig. 3.30

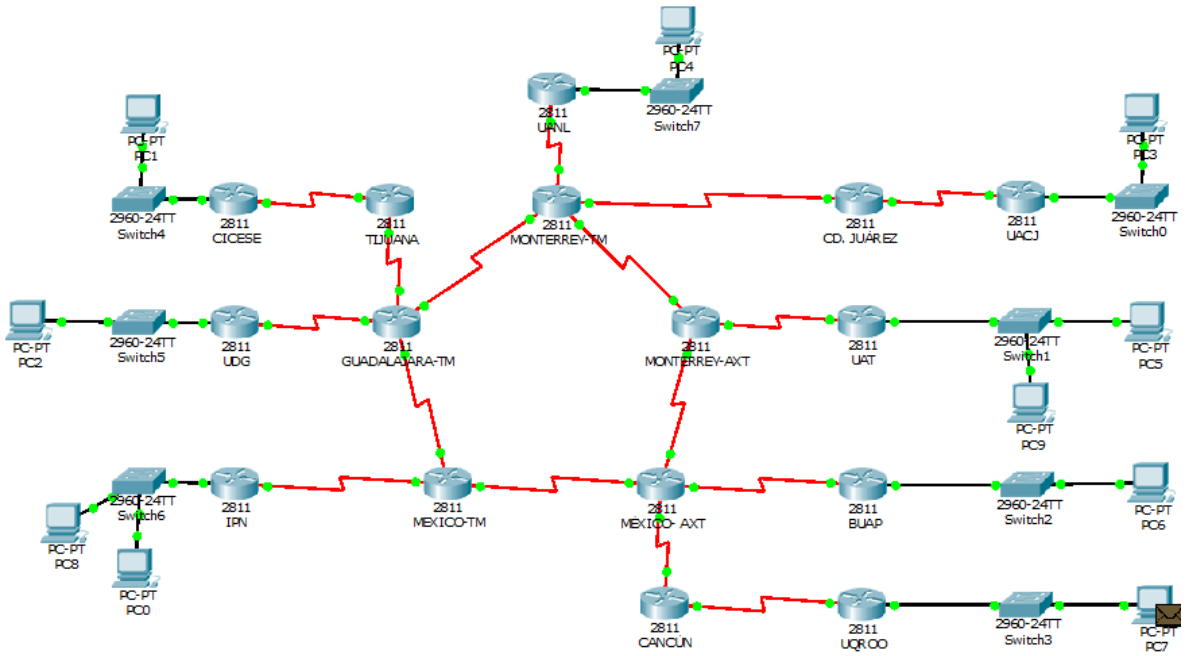

Fig. 3.30 Llegada del paquete request ICMP al host7.

Una vez que el paquete replay ICMP llega con éxito al host1 el proceso ping se ha completado, como se muestra en la fig. 3.31. En este punto el proceso ping indica que

el destino es alcanzable, por lo tanto ambos host están listos para enviar y compartir información.

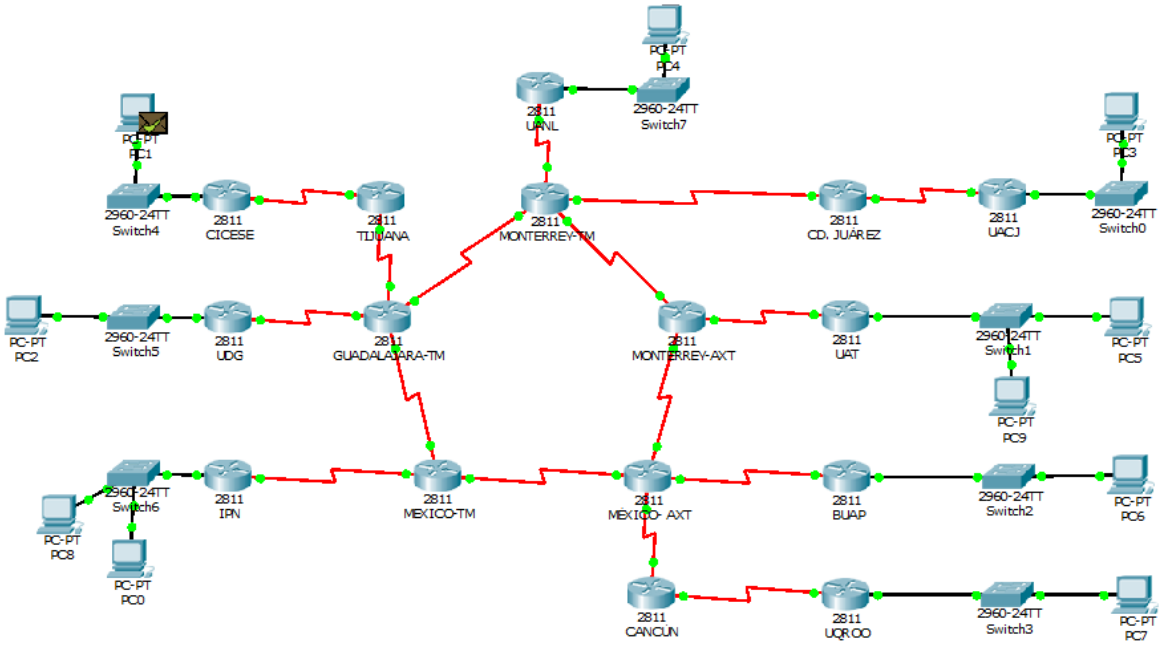

Fig. 3.31 Paquete ICMP llegando con éxito al host1.

En la fig. 3.32 a) se muestran las tramas que son enviadas por el host7 hacia el host1, b) se muestran las tramas recibidas por el host1, con lo cual finaliza el proceso ping con éxito.

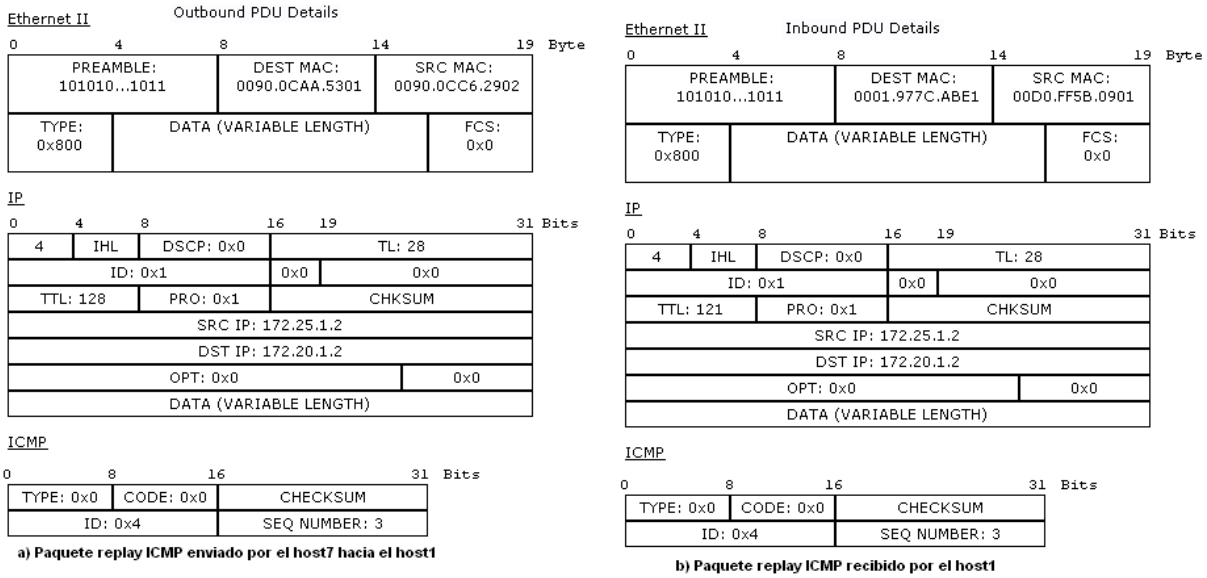

Fig. 3.32 Paquete ICMP llegando con éxito al host1.

Al enviar un ping del host1 el cual se encuentra en el router CICESE hacia el host7 UQROO con dirección IP 172.25.1.2 /16, el ping es recibido satisfactoriamente. Al enviar 4 paquetes ICMP con 32 bytes, los tiempos fueron mínimo=172 ms, promedio=239 y máximo de 312 ms.

En la fig. 3.33 se muestra el uso de CPU el cual fue del 5% y del uso de la memoria RAM de 1.70 GB, durante la simulación del backbone de la red CUDI.

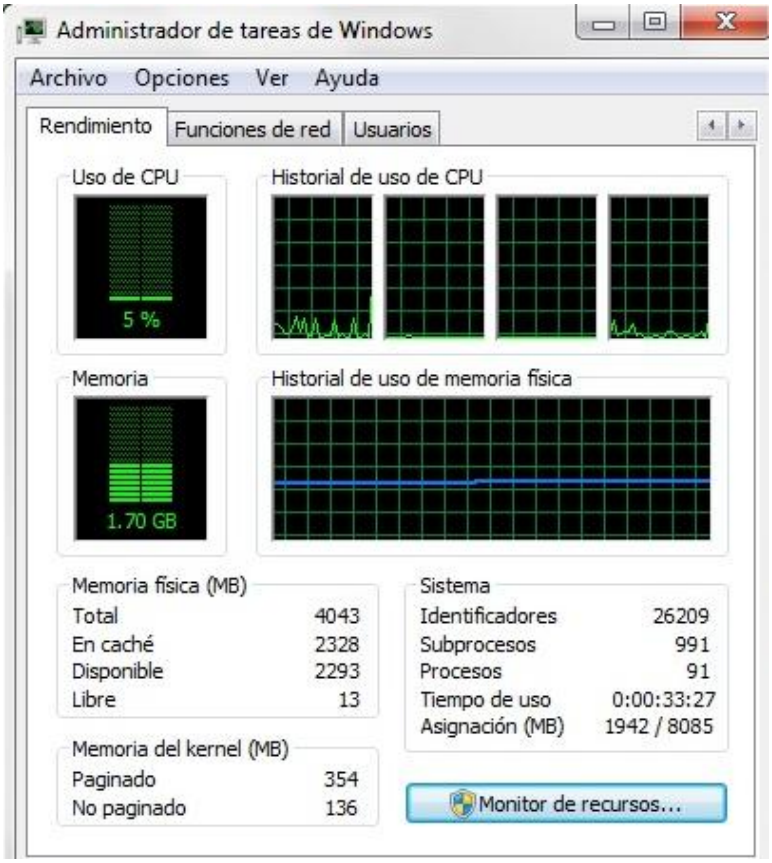

Fig. 3.33 Recursos utilizados por el simulador.

El tiempo que llevó la realización de la simulación fue de aproximadamente 7 minutos.

De la misma manera como se realizó la prueba de conectividad entre el host 1 y el host 7, se probó la conectividad entre cada uno de los 8 asociados de la red CUDI.

Tales simulaciones no se presentan dado el trabajo repetitivo y para no hacer más extenso este material.

Capítulo 4

Emulación del Backbone de la Red Avanzada I2 en México

4.1 Introducción: Emulación GNS3 v0.8.6

En este capítulo se presentan los resultados de la emulación realizada en GNS3 v0.8.6 (Graphical Network Simulator, Simulador de Redes Grafico), GNS3 es un emulador de software libre de código abierto. Las características del equipo utilizado para realizar la emulación son: Laptop HP Pavilion g4, Procesador Intel(R) Core(TM) i3-2330M CPU @ 2.20Ghz, RAM 4GB, Sistema operativo Windows 7 Home Basic, Service Pack 1, Sistema Operativo de 64 bits. Un emulador es un software que se puede ejecutar en un hardware diferente para el que fue originalmente diseñado y un simulador solo reproduce el comportamiento del software original. [Apéndice A]

En la emulación se empleó la topología de la red CUDI de la fig. 3.1, que como se mencionó anteriormente es parcial ya que sólo cuenta con el Backbone y con 8 afiliados por simplicidad.

Para la emulación se emplearon direcciones IP de clase B, con las cuales se configuraron cada una de las interfaces de los routers de la red CUDI, se utilizaron las direcciones de la tabla 3.1. Para realizar el enrutamiento se utilizaron las direcciones de red de la tabla 3.2.

Mientras que los host utilizaron las direcciones IP que se encuentran en la tabla 3.3 para que cada uno de los host se comunicaran entre ellos.

Para realizar la emulación de la Red CUDI, se emplearon routers C7200-JK9S-M con IOS v12.4 y routers 3725-ADVENTERPRISEK9-M con el módulo NM-16ESW con IOS v12.4 y host, el cual puede ser utilizado como switch. Dentro del emulador GNS3 se colocan los equipos utilizados para crear la red CUDI como se muestra en la fig. 4.1.

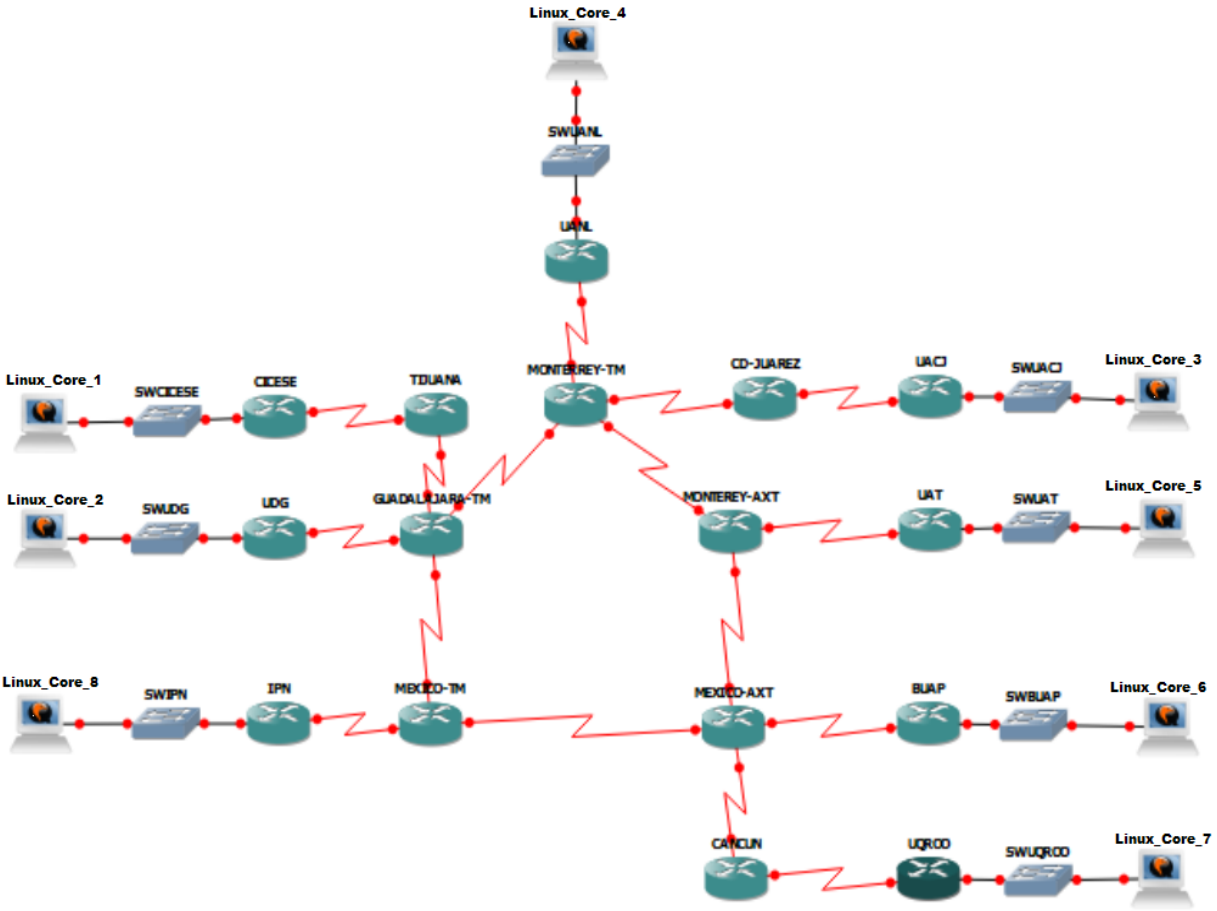

Fig. 4.1 Topología de Backbone de CUDI, creada en el emulador GNS3.

4.2 Configuración de Router

Una vez realizada nuestra red CUDI en el emulador se procede a configurar cada uno de los equipos con los que cuenta la red, empleando las direcciones IP de las tablas 3.1, 3.2 y 3.3.

En la configuración de cada uno de los routers, se deben configurar sus interfaces así como el protocolo de enrutamiento OSPF el cual es empleado por la red CUDI.

La configuración de cada uno de los routers con los que cuenta la red CUDI se configuró por medio de CLI, tal y como se haría desde la consola de un router real, todos los routers se configuraron con los mismos comandos, sólo cambiaron las direcciones IP utilizadas por los routers y sus interfaces. Para guardar la configuración en cada uno de los router se pueden utilizar los siguientes comandos: copy running-config, startup-config, write memory o wr, así no se perderá la configuración al salir

del emulador o al apagar el equipo, la fig. 4.2 muestra la configuración para el router CICESE.

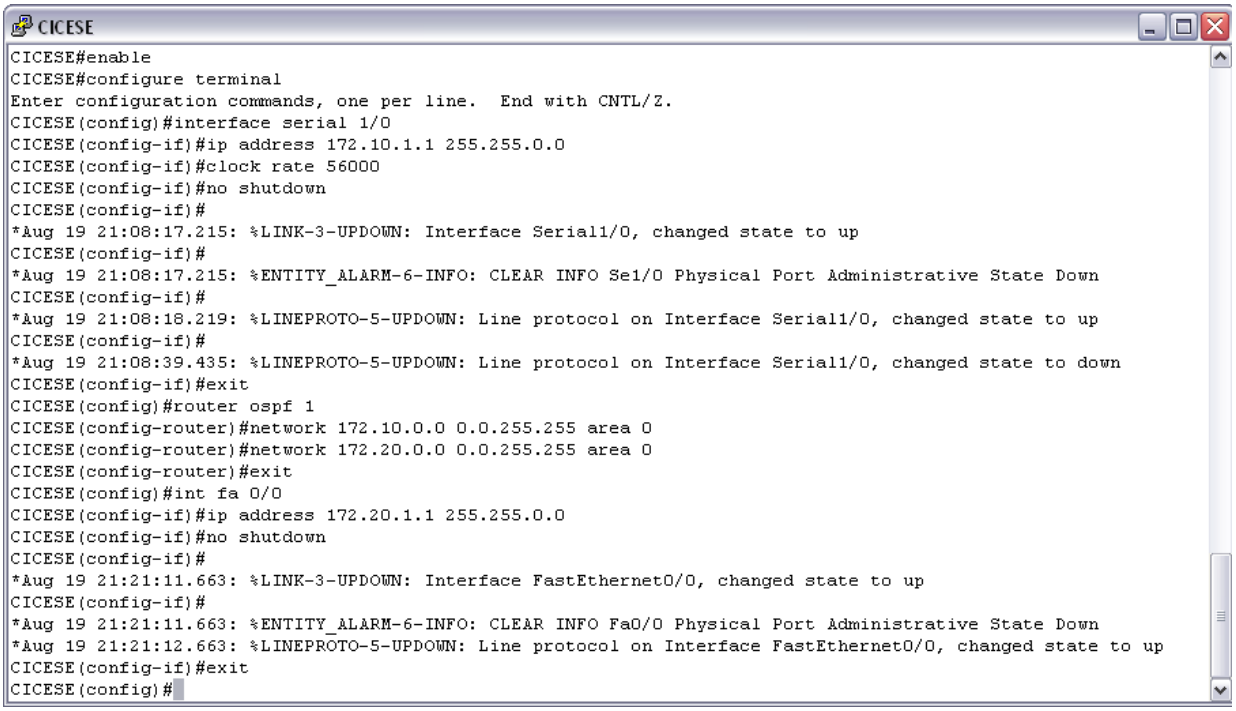

Fig. 4.2 Configuración del router CICESE en el emulador GNS3.

4.3 Configuración de Host

Enseguida se configuraron los host con las direcciones IP de la tabla 3.3 para cada uno de los host de la red CUDI, para emular los host se utilizó un Qemu (Quick EMUlator, Emulador Rápido) el cual emula imágenes de Linux para ser utilizado por los host, el Qemu utilizado fue el Linux Microcore 3.8.2. En la fig. 4.3 se muestra un ejemplo de la configuración del host CICESE a la cual se le configuró la dirección IP, la máscara de subred y el Gateway. La configuración para los host se llevó a cabo en el editor de textos “vi” para poder guardar la configuración de cada host, el editor de textos “vi” que significa “Visual” es usado por los sistemas UNIX pero LINUX lo utiliza para añadir o cambiar configuraciones, este tipo de editor utiliza operaciones sencillas basados en cursores pero no tiene la facilidad de uso como se realizaría en editores con interfaz gráfica. [96]

El editor “vi” tiene tres modos de operación para el teclado:

1. Modo comando: las teclas del teclado son comandos.
2. Modo entrada: las teclas se convierten en caracteres de entrada
3. Modo edición: algunas teclas se utilizan para cambiar de modo entrada a modo comando o de modo comando a modo entrada. [96]

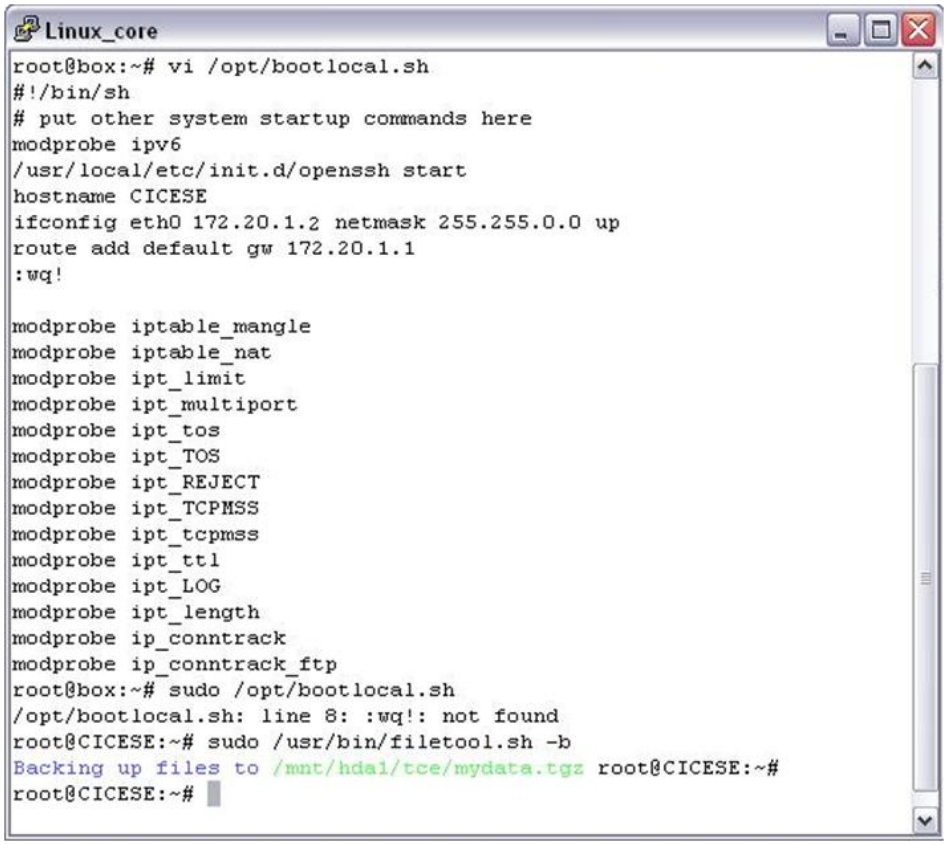

Fig. 4.3 Editor de textos vi en el emulador GNS3.

El editor de textos “vi” fue utilizado para guardar los cambios de la configuración de cada host ya que si no se utilizaba el editor de textos era imposible guardar su configuración. A continuación se muestran los pasos para guardar la configuración del host dentro del editor “vi”:

1. Primero se ingresa al modo privilegiado por medio del comando “*sudo su”*.
2. Para el acceso al editor “vi” se utiliza el comando “*vi /opt/bootlocal.sh”*.
3. A continuación se ingresan los comandos para configurar la dirección IP, la máscara de red y el gateway.

Host name CICESE

Ifconfig eth0 172.20.1.2 netmask 255.255.0.0

Route add default gw 172.20.1.1

4. En seguida se guarda la configuración con el comando "*:wq!".*
5. A continuación se hacen los cambios "*Sudo /opt/bootlocal.sh*"
6. Por último se guardan los cambios de la configuración con el comando "*sudo /usr/bin/filetool.sh –b"* y se verifican los cambios, como se muestra en la fig. 4.4.

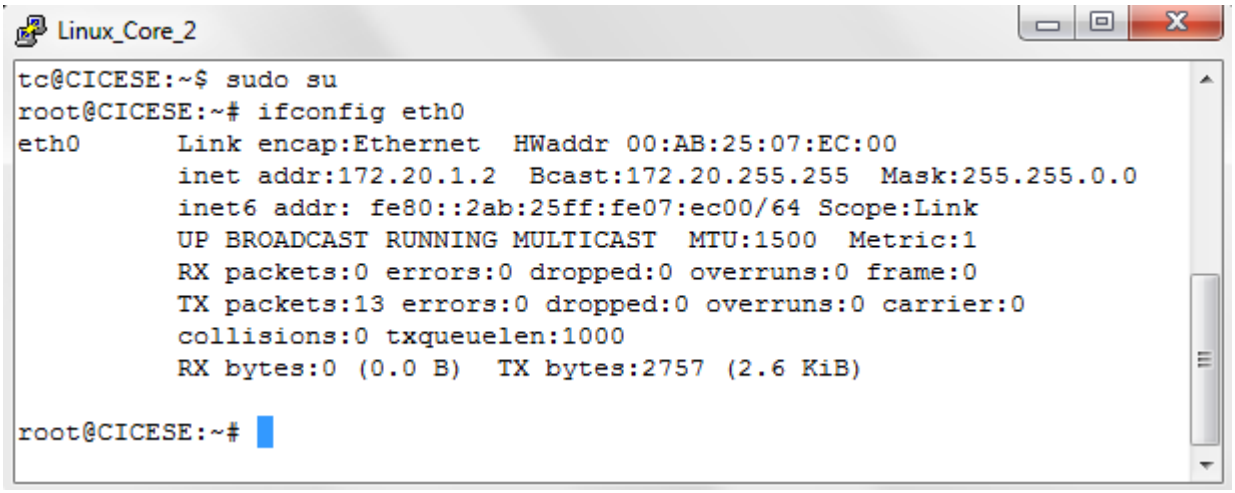

Fig. 4.4 Configuración después de realizar los cambios con el editor "vi" para que la configuración no se pierda.

Una vez realizada la configuración de cada uno de los equipos de la red CUDI se procede a realizar la emulación. Para nuestro ejemplo se envió un ping del host1 (Linux_Core_1) que se encuentra en el CICESE hacia el host7 (Linux_Core_7) que se encuentra en UQROO como se muestra en la fig. 4.5.

Para realizar la emulación primero se deben encender cada uno de los equipos de la red CUDI uno por uno, de otra manera el emulador utiliza mayores recursos de la laptop como memoria RAM y un mayor uso de CPU, cabe mencionar que aún encendiendo uno por uno los equipos se tiene un rendimiento alto de los recursos de la laptop en la que se está emulando nuestra red. Por ello una vez encendido el primer equipo se debe configurar el IDLEPC (Idle CPU, CPU virtual de un router

Inactivo) el cual es un valor que hace que el emulador ocupe menos recursos del CPU de la computadora cuando está inactivo el CPU virtual de un router emulado.

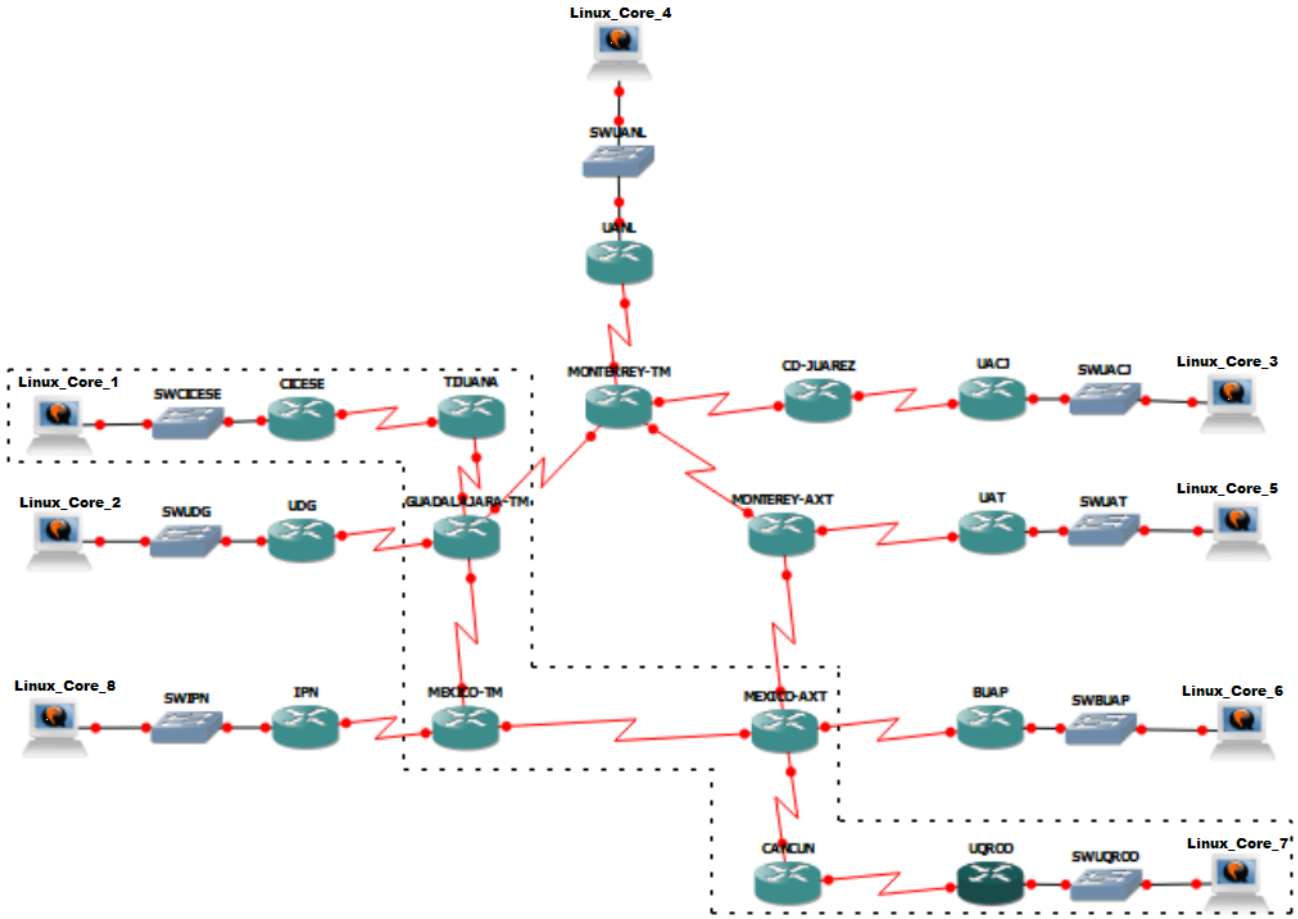

Fig. 4.5 Los equipos que se encuentran encerrados entre las líneas punteadas son los que se encuentran encendidos.

GNS3 realiza un análisis del equipo encendido y verifica la imagen de IOS con el que cuenta para determinar el mejor valor de IDLEPC a utilizar, una vez determinado el valor de IDLEPC se selecciona este valor y se continúa con el encendido de cada uno de los equipos. En la fig. 4.6 se muestra el rendimiento de CPU utilizado durante la emulación, cabe mencionar que sólo los equipos encendidos son los de la ruta del host1 al host 7, encerrados entre líneas punteadas como se muestra en la fig. 4.5.

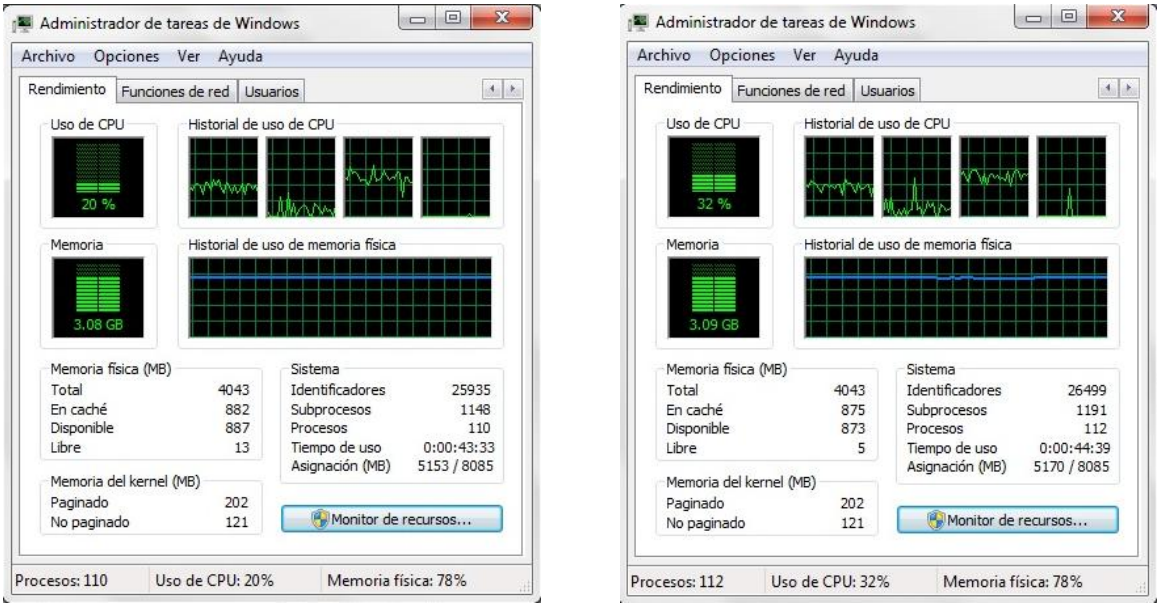

Fig. 4.6 Uso del rendimiento del CPU durante la emulación el cual varía del 20% al 32%.

Al enviar un ping del host1 el cual se encuentra en el CICESE hacia el host7 UQROO con dirección ip 172.25.1.2 /16, en la fig. 4.7 se muestra que el ping fue recibido satisfactoriamente al enviar 5 paquetes de 56 bytes de datos más 8 bytes de cabecera ICMP lo que da un total de 64 bytes, los tiempos fueron mínimo=112.576 ms, promedio=152.194 y máximo de 192.947 ms. Se enviaron 5 paquetes ya que es mucho mejor enviar una serie de 5 paquetes para tener la certeza de que los paquetes han sido recibidos satisfactoriamente, sin embargo se pueden enviar los paquetes de ping que se deseen.

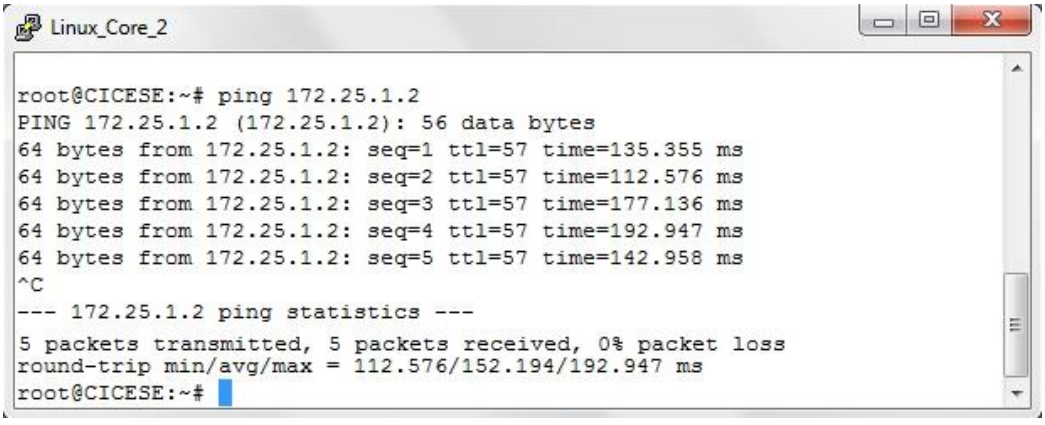

Fig. 4.7 Ping enviado al host7 UQROO el cual fue exitoso.

En seguida se envía un ping del host7 que se encuentra en UQROO hacia el host1 que está en el CICESE con dirección ip 172.20.1.2 /16, en la fig. 4.8 se muestra que el ping fue recibido satisfactoriamente al enviar 5 paquetes de 56 bytes más 8 bytes de cabecera ICMP lo que da un total de 64 bytes, los tiempos fueron mínimo=91.036 ms, promedio=114.021 ms y máximo de 161.138 ms.

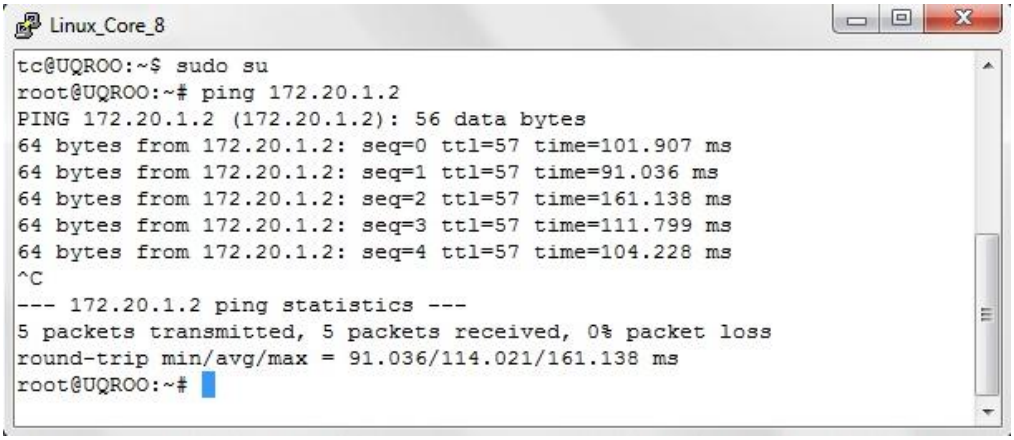

Fig. 4.8 Ping enviado al host CICESE el cual fue exitoso.

4.4 Monitoreo

Para visualizar los tipos de paquetes que son enviados al realizar un ping del host1 al host7 utilizamos un analizador de paquetes o de protocolos "*sniffers*" los cuales se encargan de supervisar, analizar y llevar estadísticas del comportamiento de nuestra red, utilizado el sniffer Wireshark, se observa que al realizar el ping con Wireshark podemos ver los ICMP request y replay los que son requeridos por el proceso ping, como se muestra en la fig. 4.9. [97] [98]

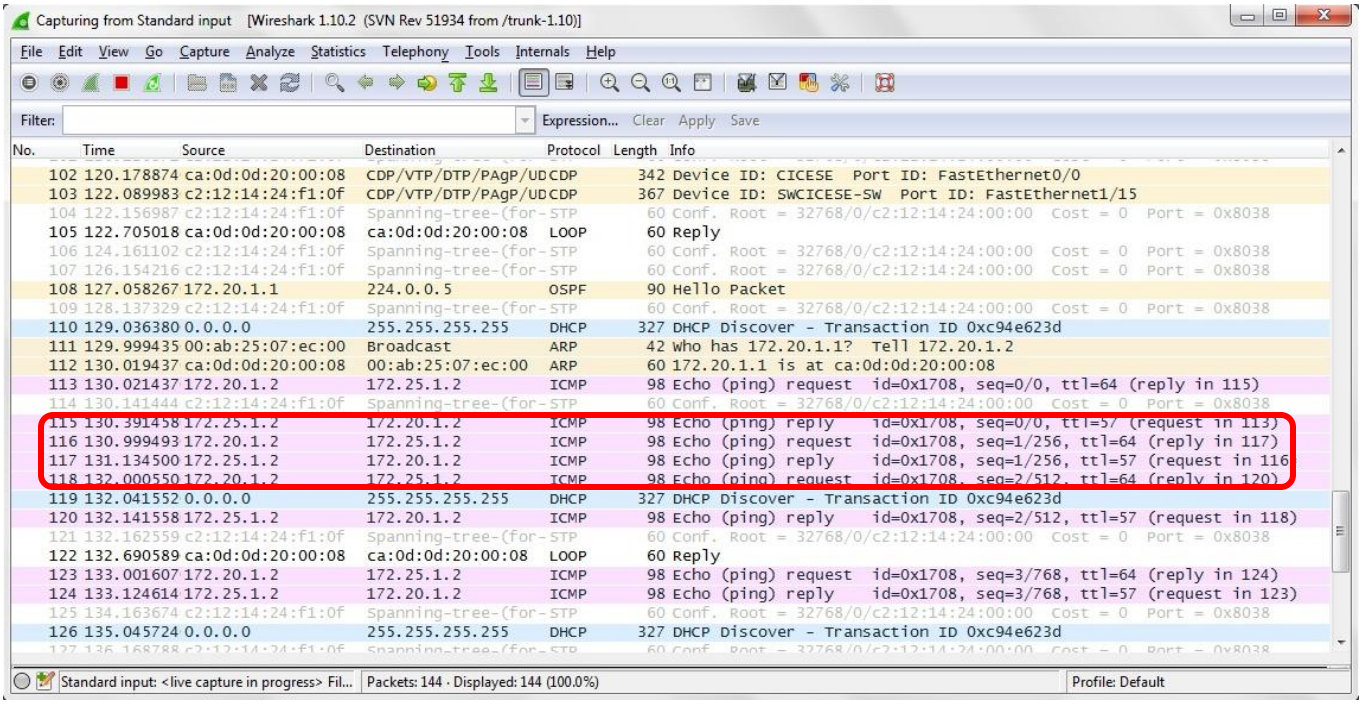

Fig. 4.9 Sniffer Wireshark para visualizar el ICMP.

Con el sniffer Wireshark se pueden ver también los paquetes HELLO del protocolo OSPF para descubrir a sus vecinos, como se muestra en la fig. 4.10.

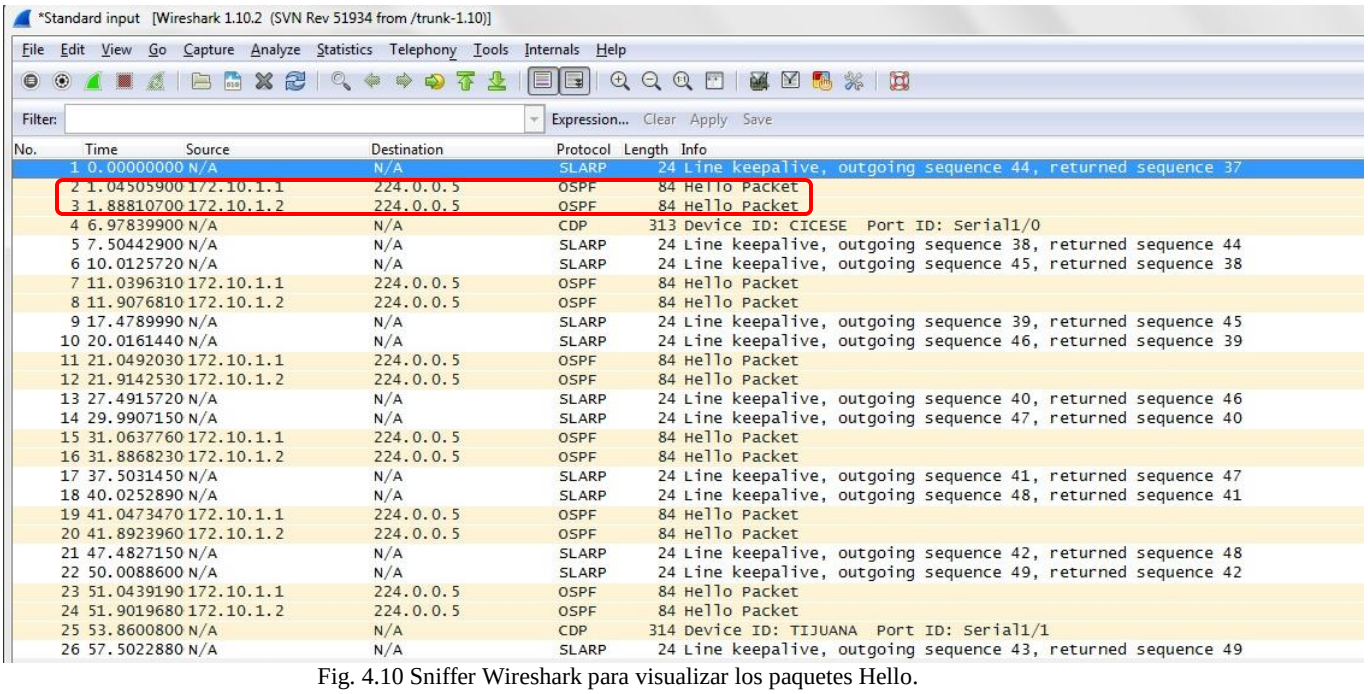

Fig. 4.10 Sniffer Wireshark para visualizar los paquetes Hello.

Con la finalidad de verificar la correcta configuración de OSPF, se muestra a continuación para el caso del router CICESE los comandos empleados. Estos mismos pueden ser empleados por otros router para su verificación:

El comando *show ip protocols*, muestra los parámetros sobre los temporizadores, los filtros, la métrica, las redes y otra información del router, como se muestra en la fig. 4.11.

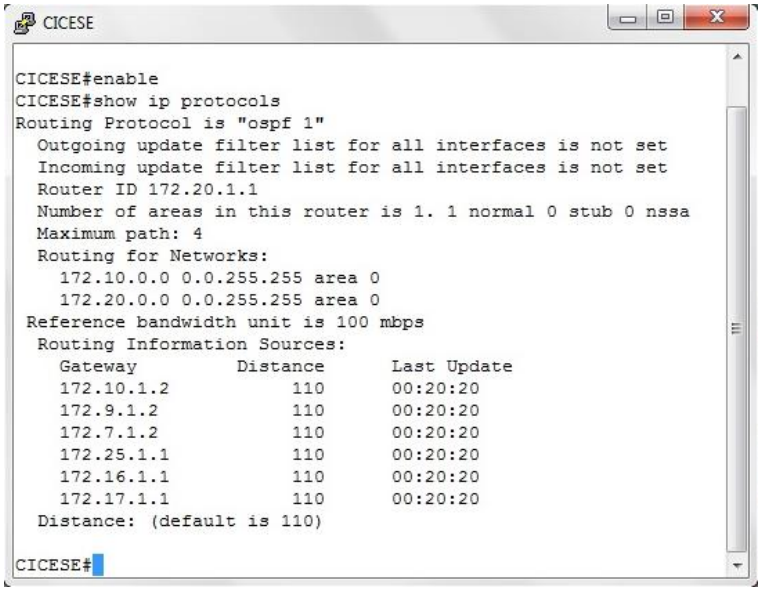

Fig. 4.11 El comando show ip protocols muestra información de ospf.

El comando *show ip route*, muestra las rutas conocidas por el router y las interfaces a través de las cuales fue posible conocerlas, como se muestra en la fig. 4.12.

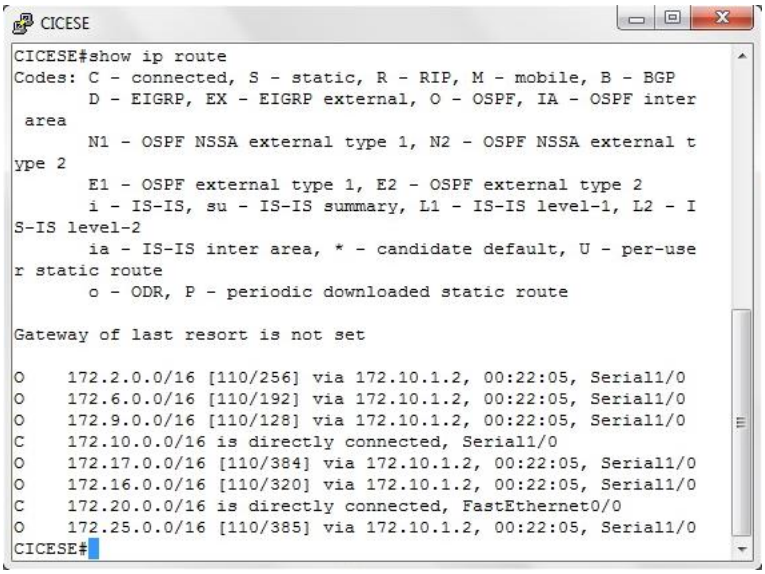

Fig. 4.12 El comando show ip route, mostrando todas las rutas del router CICESE.

El comando *show ip route ospf*, muestra estrictamente rutas ospf que obtuvo de la base de datos de adyacencia, como se observa en la fig. 4.13.

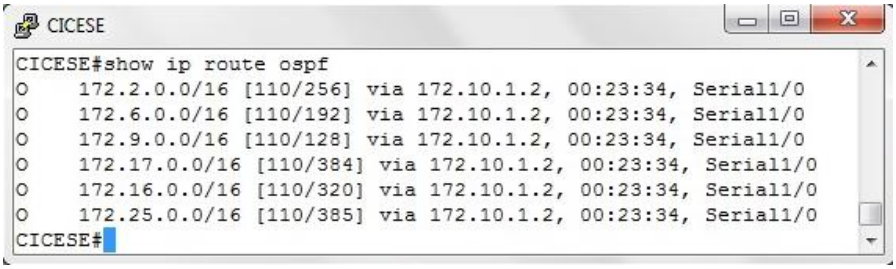

Fig. 4.13 El comando show ip route ospf, mostrando rutas OSPF.

El comando *show ip ospf interface*, verifica que las interfaces han sido configuradas en su área correspondiente, muestra la dirección ip, pero si no la tuviera indicará la interfaz que tenga la dirección más alta y se tomará como id del router, muestra intervalos de temporizador y muestra adyacencias de vecindad fig. 4.14.

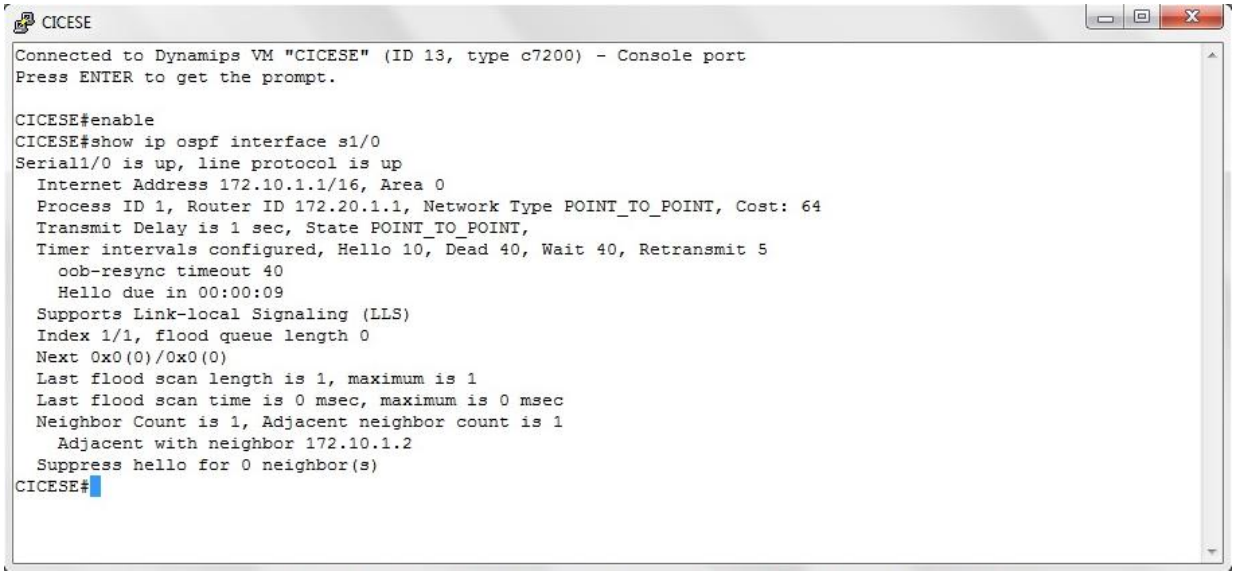

Fig. 4.14 El comando show ip ospf interface, verificando la interfaz S1/0.

El comando *show ip ospf*, muestra el número de veces que se ha ejecutado el algoritmo ospf, como se muestra en la fig. 4.15.

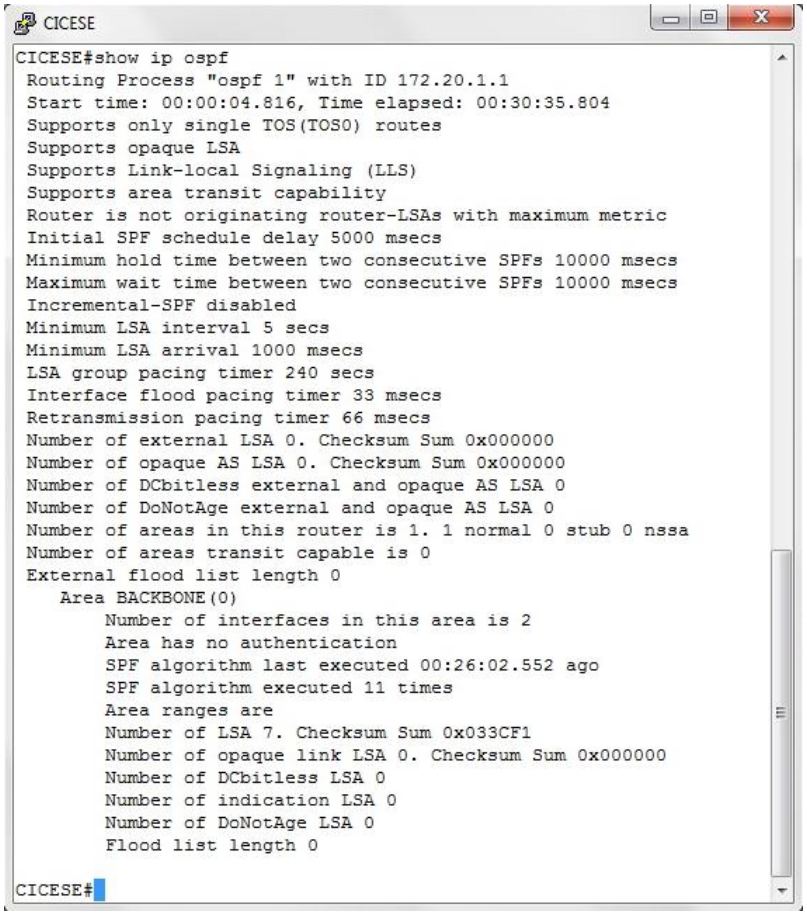

Fig. 4.15 El comando show ip ospf, verificando la ejecución de SPf, la cual fue de 11 veces.

El comando *show ip ospf neighbor*, muestra información de vecindad OSPF sobre una base interfaz a interfaz, en la fig. 4.16 se ve la ejecución de este comando.

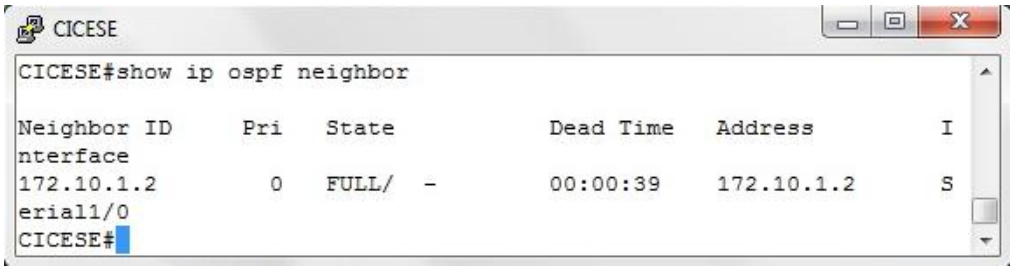

Fig. 4.16 El comando show ip ospf neighbor, mostrando la vecindad para el router CICESE.

El comando *show ip ospf neighbor detail*, muestra una lista detallada de vecinos, sus prioridades y su estado, en la fig. 4.17 se muestra la ejecución de este comando.

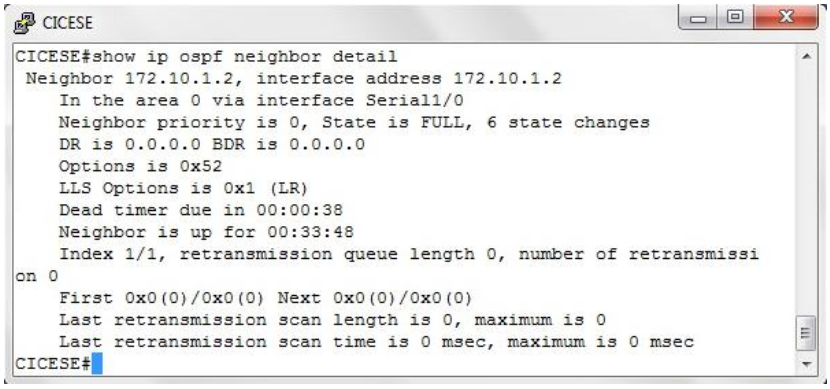

Fig. 4.17 El comando show ip ospf neighbor detail, mostrando el área y la interfaz a través del cual conoció a su vecino.

El comando *show ip ospf database*, muestra el contenido de la base de datos de topología, también muestra el id del router y el id de proceso ospf, en la fig. 4.18, se muestra la ejecución de este comando.

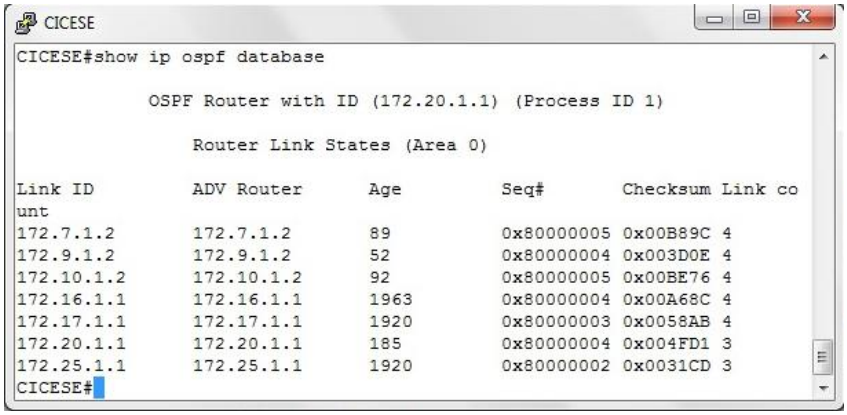

Fig. 4.18 El comando show ip ospf database, base de datos de topología obtenida a través del algoritmo SPF.

De la misma manera, se probó la conectividad entre cada uno de los afiliados, se realizó la prueba de conectividad entre los host 1 y host 7, así como también la verificación de la configuración de OSPF para cada router de la red CUDI, estas emulaciones no se presentan dado que es repetitivo y el material se haría más extenso.

4.5 Caracterización del rendimiento del sistema de emulación

Para conocer qué tantos recursos consume el emulador GNS3 se deben tomar en cuenta las características del equipo, las cuales son: Laptop HP Pavilion g4, Procesador Intel(R) Core(TM) i3-2330M CPU @ 2.20 Ghz, RAM 4 GB, Sistema operativo Windows 7 Home Basic, Service Pack 1, Sistema Operativo de 64 bits, debido a que el emulador GNS3 utiliza recursos físicos como el uso de CPU y de la memoria RAM. A continuación se procede a encender cada uno de los router de la red CUDI de la fig. 4.1. Primero se encienden los equipos de la ruta de CICESE – UQROO, ha esta ruta se le agregan los equipos de las siguientes rutas como sigue: ruta IPN + UDG + ruta Monterrey – ruta UANL + ruta Cd. Juárez + ruta Monterrey AXT + ruta BUAP, de la ruta BUAP faltaron encender dos equipos, el host 6 y el SWBUAP, por lo que de un total de 32 equipos solo se encendieron 30 equipos, con ello los recursos que consume el emulador son el 100% del uso del CPU y 3.16 GB de memoria RAM de un total de 4 GB, en la tabla 4.1 se muestran los resultados obtenidos del administrador de tareas, del uso de recursos de la laptop en la que se realizó la emulación.

Ruta	Número de equipos (Router, Switch, host)	Uso del CPU %	Memoria RAM utilizada GB
CICESE – UQROO	(7+2+2)=11	32	3.08
UDG	(1+1+1)=3 (11+3=14)	33	3.10
IPN	(1+1+1)=3 (14+3=17)	41	3.12
MONTERREY – UANL	(2+1+1)=4 (17+4=21)	54	3.09
CD. JÚAREZ	(2+1+1)=4 (21+4=25)	68	3.13
MONTERREY AXT	(2+1+1)=4 (25+4=29)	84	3.15
BUAP	(1+0+0)=1 (29+1=30)	100	3.16
	Total de equipos emulados 11+3+3+4+4+4+1=30	100% de 100% del uso de CPU	3.16GB de 4GB de memoria RAM utilizada

Tabla 4.1 Recursos utilizados por el emulador GNS3

El tiempo en el que se llevó la realización de la emulación fue alrededor de aproximadamente 1 hora, esto debido a que se fueron encendiendo cada uno de los equipos uno por uno y en el caso de los router se tenía que calcular el valor de IDLEPC para cada router, lo cual permitía un menor uso de recursos de la computadora.

En la fig. 4.19 se muestra la gráfica con el número de equipos que se fueron encendiendo para la emulación, también se observa que conforme aumenta el número de equipos va aumentando el uso del CPU utilizado por el emulador, también se observa que conforme aumenta el número de equipos aumenta el uso de la memoria RAM de la laptop utilizada para la emulación, para realizar la emulación sólo se ejecutaba el emulador de GNS3 y el administrador de tareas para ver los recursos utilizados esto para tener un mejor rendimiento de los recursos a utilizar de la laptop.

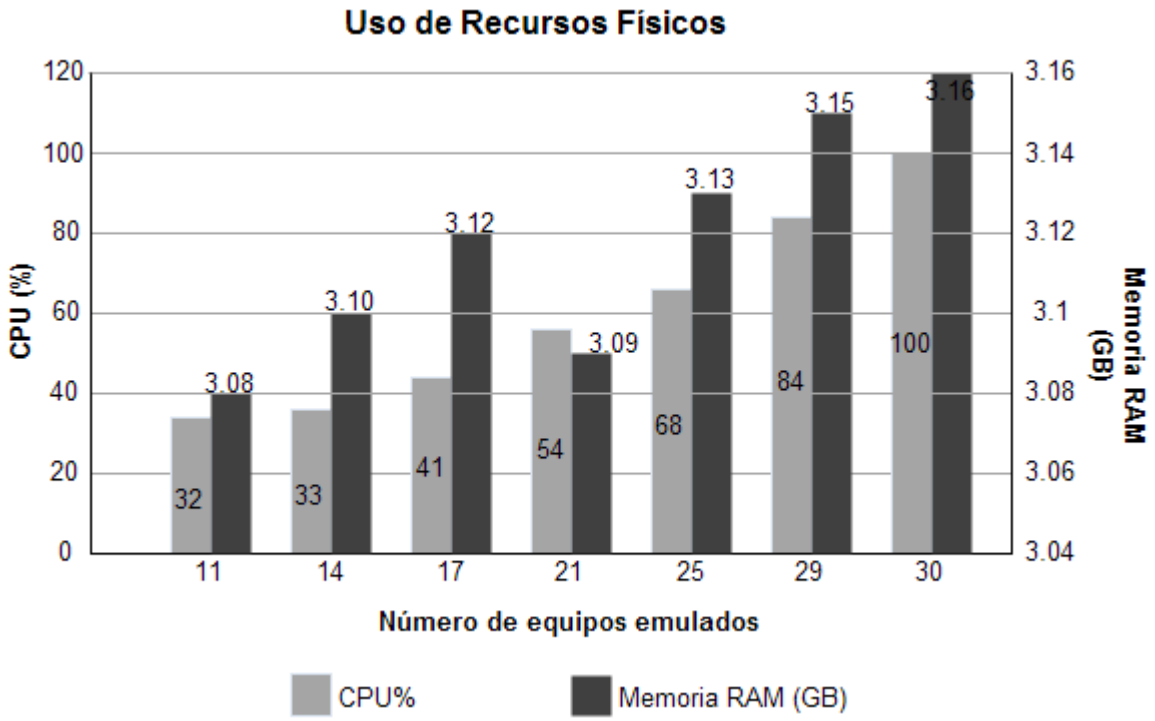

Fig. 4.19 Recursos Físicos utilizados por el emulador.

Capítulo 5

CONCLUSIONES

Desde el nacimiento de Internet en la década de los 60 en USA, Internet se ha convertido hoy en día en una herramienta más de la que dependen las personas, esto llevó a que en 1998 universidades y centros de investigación desarrollaran lo que hoy se conoce como internet 2 (I2) en USA y años después en el resto del mundo, en México se desarrollo I2 el cual es llamado CUDI (Corporación Universitaria para el Desarrollo de Internet 2. En este trabajo se realizó la "*Emulación del Backbone de la Red Avanzada I2 en México*" la cual se creó el 8 de abril de 1999.

Con base en los resultados obtenidos en la simulación se puede concluir que:

1. Se pudo conocer cómo está constituida toda su infraestructura de telecomunicaciones de CUDI, ya que su backbone cuenta con routers a nivel core y las velocidades con las que opera (STM-1, E3) esta red de I2.

2. La finalidad de simular el Backbone parcial de la red CUDI por medio del simulador Packet Tracer V5.3 de Cisco es conocer si es viable simular una red de estas características.

   - Packet Tracer V5.3 no cuenta con equipos a nivel core como el router 7200 y el switch SW-PBX 8600, por lo cual la simulación se tuvo que realizar con los siguientes equipos: routers 2811 y Switches WS-C2960-24TT.

   - Los routers 2811 soportan enrutamiento dinámico, para su configuración se utilizó el protocolo de enrutamiento OSPF, los routers 2811 soportan velocidades de STM-1 como también E3.

   - Se comprobó la conectividad al enviar ping del host1 que se encuentra en el CICESE al host 7 que se encuentra en UQRRO, el cual fue exitoso, de la misma manera se realizó lo mismo para cada uno de los demás host de los 8 afiliados. Se observaron gráficamente los paquetes ICMP así como los paquetes ARP, los cuales son utilizados al realizar ping.

   - El mismo simulador (Packet Tracer V5.3) tuvo algunos retrasos esto ocasionado por su buffer, el cual se desbordaba y tardaba algunos minutos en que se limpiara para seguir con la simulación.

   - Los recursos utilizados por el simulador fueron: uso de CPU del 5% de 100% y uso de la memoria RAM de 1.70 Gb de un total de 4 GB, ocupando pocos recursos de la computadora. La simulación se realizó aproximadamente en alrededor de 7 minutos a 10 minutos.

Con base en los resultados obtenidos en la emulación se puede concluir que:

1. Se pudo conocer como está constituida toda su infraestructura de telecomunicaciones de CUDI ya que en su backbone cuenta con router a nivel core y las velocidades con las que opera (STM-1, E3) esta red de I2.

2. La finalidad de Emular el Backbone de la red CUDI por medio de GNS3 V0.8.6 es conocer si es viable emular una red de estas características para tener una aproximación parecida a la real.

   - GNS3 V8.6 soporta IOS de routers Cisco a nivel core, pero no soporta IOS de switches, esto se contrarresta utilizando algunos routers que cuentan con módulos para ser utilizados como switches, además de que se puede conectar con equipos reales. En la emulación se utilizaron los IOS de los siguientes routers: C7200-JK9S-M IOS v12.4 y el 3725-ADVENTERPRISEK9-M con modulo NM-16ESW con IOS v12.4 utilizado como switch.

   - GNS3 soporta VMWare, VirtualBox VirtualPC, QEMU, para permitir emular varios sistemas operativos.

   - Los routers C7200 soportan enrutamiento dinámico, para su configuración se utilizó el protocolo de enrutamiento OSPF, la cual se realizo por medio de CLI.

   - Los routers C7200 soportan velocidades de STM-1, como también E3.

   - Se utilizó el emulador QEMU (Linux Microcore 3.8.2) debido a que es una emulación de Linux, en el que se configuraron su dirección de red, su máscara de red y el gateway por medio del editor Vi.

   - El arranque de la emulación se lleva encendiendo equipo por equipo de la red CUDI, por que el emulador utiliza recursos físicos de la computadora, para lo cual se configura el valor de IDLEPC de los equipos para tener un mejor rendimiento.

   - Se comprobó la conectividad al enviar ping del host1 que se encuentra en el CICESE al host 7 que se encuentra en UQRRO, el cual fue exitoso, de la misma manera se realizó lo mismo para cada uno de los demás host afiliados.

   - No se pueden ver gráficamente los paquetes ICMP ni los paquetes ARP, los cuales son utilizados al realizar ping, sin embargo, GNS3 utiliza el sniffer o analizador de protocolos Wireshark, con el cual se observaron los ICMP request y reply al realizar ping, también se observaron los paquetes HELLO los cuales son utilizado por el protocolo de enrutamiento OSPF para descubrir a sus vecinos.

- El emulador (GNS3 V8.6) tardaba algunos minutos en ir encendiendo cada uno de los equipos, esto debido a que cada uno de los equipos utilizaba recursos físicos de la computadora.

- Los recursos utilizados por el emulador fueron: uso de CPU del 100% de 100% y uso de la memoria RAM de 3.16 Gb de un total de 4 GB, ocupando una gran cantidad de recursos físicos de la computadora. La simulación se realizó aproximadamente en alrededor de 1 hora.

Tanto el simulador (Packet Tracer v5.3) de Cisco como el emulador (GNS3 v0.8.6) fueron capaces de soportar el backbone de la red CUDI , cada uno con las observaciones antes mencionadas, destacando que el simulador no cuenta con los equipos a nivel core, mientras que su bufer se llena y necesita ser limpiado, pero ocupando menores recursos físicos de la computadora, en tanto el emulador utiliza los IOS de los equipos reales, los cuales deben de ser configurados con un valor de IDLEPC adecuado para ocupar menos recursos físicos. El emulador ocupa mayores recursos físicos de la computadora, pero este se aproxima más a la red real, se recomienda utilizar una computadora que cuente con mayores recursos físicos para poder acercar aun más el backbone de la red CUDI emulado a lo real.

La dificultad de implementar una red avanzada de este tipo en laboratorio es que solamente las empresas de telecomunicaciones que son ISP (Internet Service Provider, Proveedor de Servicios de Internet) o CSP (Communications Service Provider, Proveedor de Servicios de Comunicaciones) cuentan con este tipo de equipo (como: routers a nivel core) por su precio. Por ello, este trabajo representa una opción para analizar este tipo de redes.

Habilidades adquiridas en cursos:

- Capacidad de análisis en redes de acceso.
- Manejo de simulador Cisco packet tracer nivel básico.

Habilidades adquiridas en este trabajo:

- Capacidad de análisis en redes de acceso.
- Manejo de simulador Cisco packet tracer nivel avanzado.
- Manejo de emulador GNS3 y herramientas asociadas intermedio.
- Manejo de equipo de backbone Cisco 7200 como el empleado en CUDI.
- Cuando se configura un Cisco 7200 (router core), [WAN, MAN Aggregation for Industry] nos podemos percatar de que GNS3 emula de manera idéntica al equipo de backbone.

APÉNDICE A
Instalación De GNS3

A.1 Introducción

GNS3 (Graphical Network Simulator) es un software de emulación gráfica que permite la creación y configuración de redes virtuales, GNS3 se ejecuta desde una PC, el cual soporta IOS (Internetwork Operation System) de CISCO para la emulación de los routers, también soporta VMWare, virtualBox, virtualPC, Qemu, Pemu, los cuales permiten emular varios sistemas operativos como Windows XP o LINUX.

GNS3 requiere de la instalación de los IOS, en la tabla A.1 se muestran los IOS soportados por el emulador, así como de los programas de emulación para crear emulaciones de redes de datos. [99]

IOS Cisco					
1	1700	10	2610XM	19	2691
2	1710	11	2611	20	3600
3	1720	12	2611XM	21	3620
4	1721	13	2620	22	3640
5	1750	14	2620XM	23	3660
6	1751	15	2621	24	3725
7	1760	16	2621XM	25	3745
8	2600	17	2650XM	26	7200
9	2610	18	2651XM	27	7206

Tabla A.1 IOS de CISCO que soporta GNS3 sin incluir versión.

GNS3 utiliza principalmente 3 emuladores para crear las emulaciones de las redes:

1. Dynamips: es encargado de emular los routers CISCO y el encargado de ejecutar las imágenes de los IOS de los routers que se le han instalado.
2. VirtualBox: es un virtualizador, el cual permite ejecutar diferentes sistemas operativos.
3. Qemu: es el emulador de Host de código abierto.

GNS3 puede ser instalado en diversos sistema operativos Windows, Linux y MacOS, a continuación se realiza la explicación de la instalación de GNS3 para Windows.

A.2 Instalación de GNS3

1. Paso: Descargar GNS3-0.8.6 para Windows de la siguiente página de internet: http://www.gns3.net/download/# . El archivo a descargar es **GNS3 v0.8.6 all-in-one,** la fig. A.1 muestra la descarga de GNS3.

Fig. A.1 Ventana que muestra la descarga de GNS3 7200.

2. Paso: Una vez descargado GNS3 seleccionamos ejecutar ver fig. A.2, enseguida aparecerá una ventana de configuración de la instalación y aceptamos la licencia.

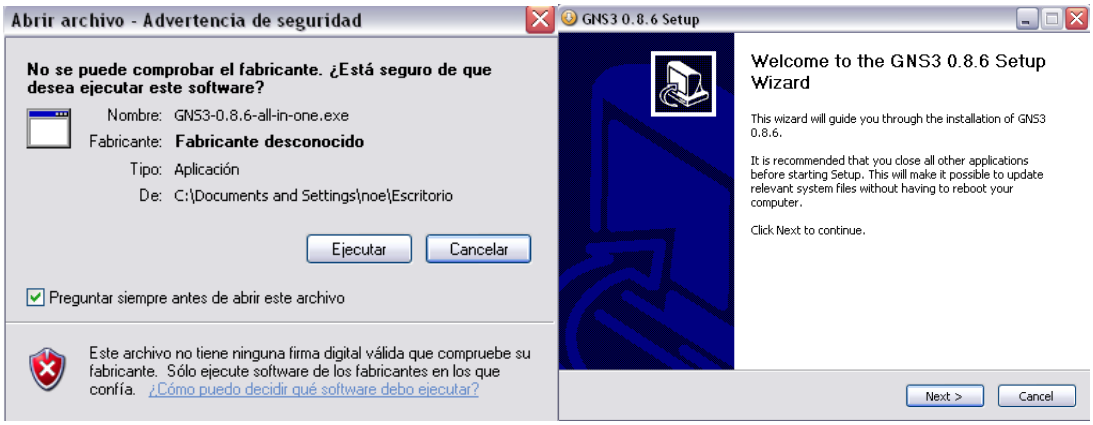

Fig. A.2 Ventana para comenzar la instalación de GNS3.

3. Paso: Saldrá una ventana donde crea un folder que se llamará GNS3, como se

muestra en la fig. A.3.

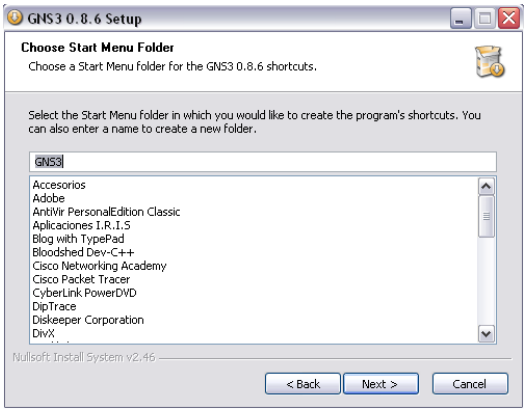

Fig. A.3 Ventana que muestra la creación de la carpeta GNS3.

4. Paso: La fig. A.4 muestra varios programas de los que depende GNS3 para funcionar. Como: WinPCAP, un software de filtrado que permite capturar y transmitir paquetes de la red permitiendo acceder fácilmente a las capas de red de bajo nivel; Dynamips, un software que se encarga de emular los IOS de CISCO en la PC, Qemu es un software que emula software de sistemas operativos de código abierto, Pemu es un software que emula los firewall de CISCO; VPCS (Virtual PC Simulator) es un simulador virtual de pc sencillo el cual se utiliza para probar la comunicación de la red enviando ping. Los programas anteriormente mencionados están seleccionadas por defecto para la instalación, para continuar seleccionamos el botón siguiente.

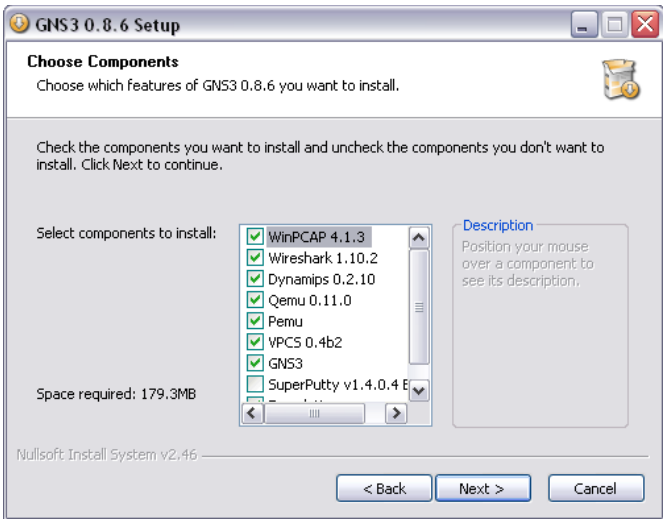

Fig. A.4 Ventana que muestra las aplicaciones utilizadas por GNS3.

5. Paso: A continuación comenzará la instalación de GNS3 en la ruta predeterminada, seleccionar Install para continuar, como se muestra en la fig. A.5.

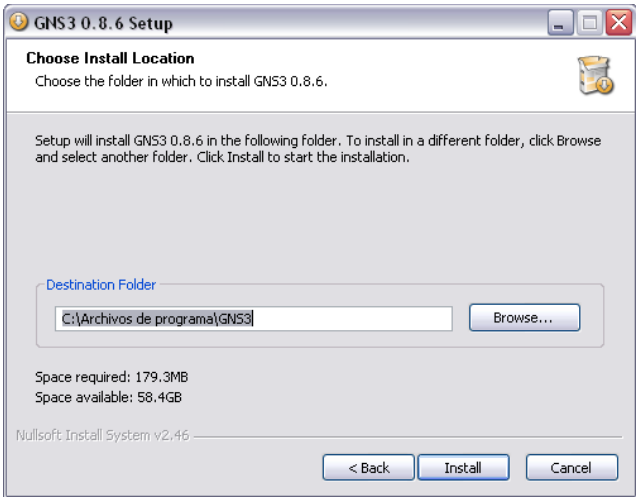

Fig. A.5 Ventana que muestra donde será instalado GNS3.

6. Paso: Se abrirá una ventana de instalación de WinPcap, como se muestra en la fig. A.6. Posteriormente saldrá una nueva ventana la cual aceptamos los términos de licencia de WinPcap, para continuar con la instalación.

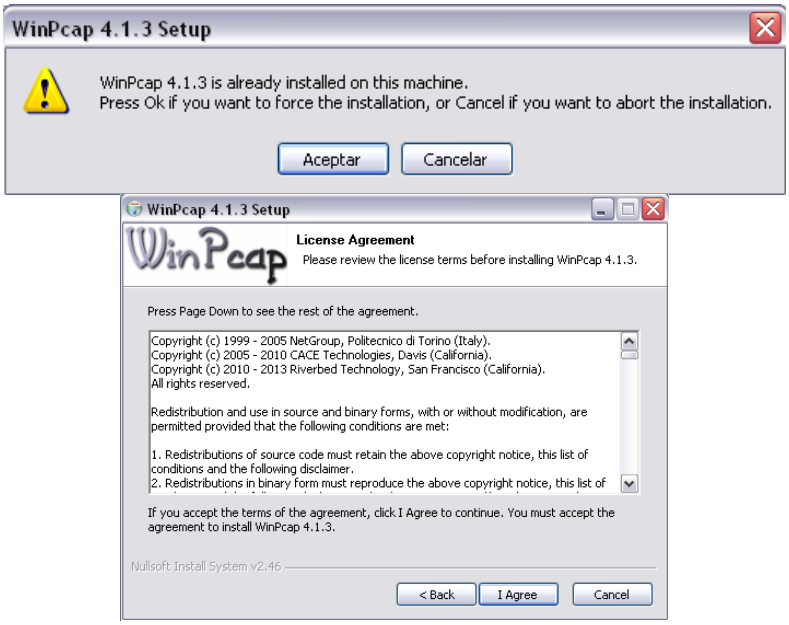

Fig. A.6 Ventana que muestra el inicio de la instalación de WinPcap.

7. Paso: Después de instalado WinPcap, continua la instalación de Wireshark 1.10.2. Wireshark es un analizador de protocolos, que se encarga de analizar el tráfico que hay en la red permitiendo examinar los datos capturados, wireshark está bajo licencia libre y se puede instalar en diversos sistemas operativos, en la fig. A.7 se muestra el inicio de la instalación.

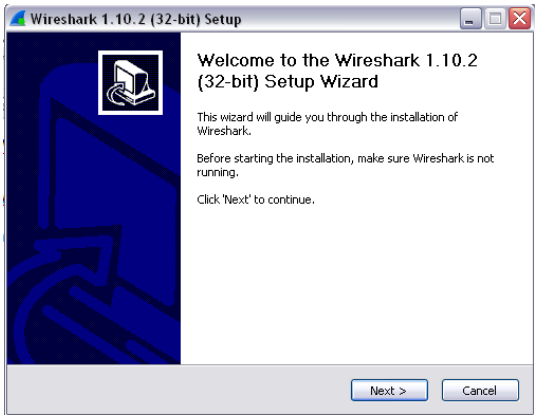

Fig. A.7 Ventana que muestra el inicio de instalación de Wireshark.

8. Paso: Después de instalado Wireshark, se continúa la instalación de GNS3, fig A.8.

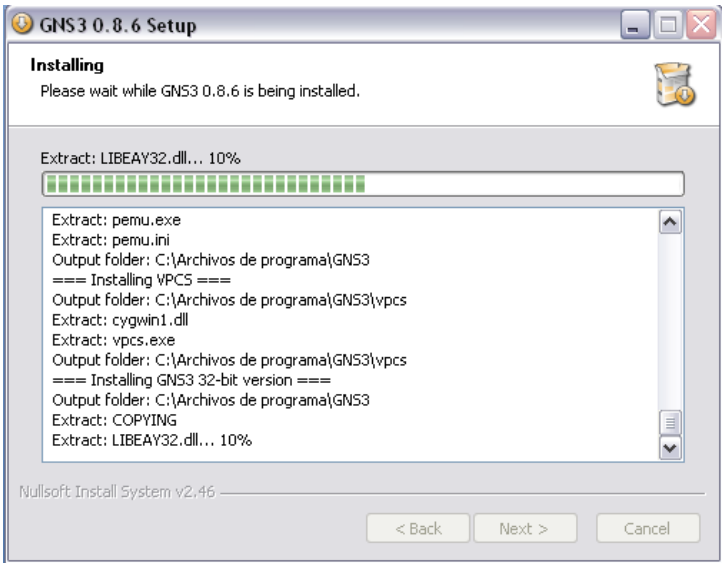

Fig. A.8 Ventana que muestra la instalación de GNS3.

9. Paso: La fig. A.9 muestra la finalización de la instalación de GNS3.

Fig. A.9 Ventana que muestra la finalización de la instalación de GNS3.

10. Paso: GNS3 se inicia automáticamente la primera vez, mostrando su ventana principal de GNS3 y una subventana para configuraciones que se encuentran marcadas por tres casillas, como se presenta en la fig. A.10.

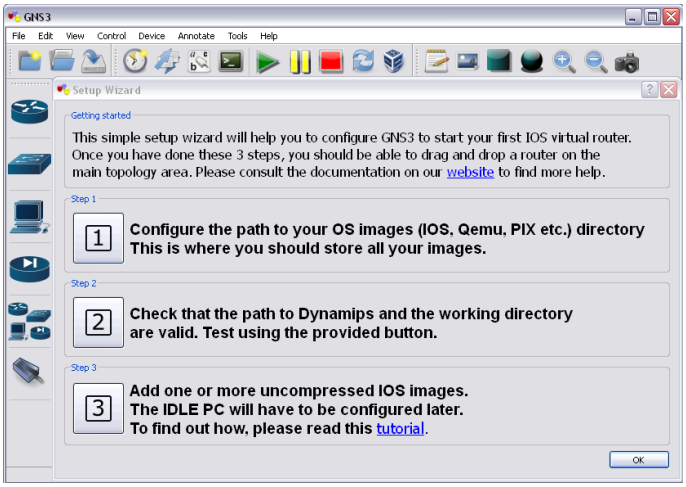

Fig. A.10 Ventana principal de GNS3.

11. Paso: Configuración de la ubicación de los IOS. Primero se debe crear una carpeta en mis documentos llamada GNS3, dentro de esta carpeta se crea una nueva carpeta llamada IOS en donde se tendrán todos los IOS de Cisco que se vayan a utilizar, se crea otra carpeta dentro de la carpeta GNS3 llamada proyectos. Del siguiente enlace se puede descargar la imagen de IOS del

router 7200. http://www.mediafire.com/download/cwc1h4jnjjy/c7200-advipservicesk9-mz.124-4.T1.bin

12. Paso: En la subventana que aparece se escoge la primera casilla, saldrá una ventana en la cual se coloca la ubicación de las carpetas “C:\Documents and Settings\noe\Mis documentos\GNS3\PROYECTOS” y la ubicación de “C:\Documents and Settings\noe\Mis documentos\GNS3\IOS” creadas anteriormente, esto se hace por que GNS3 buscará aquí los IOS y guardará nuestros proyectos que realicemos, la fig. A.11 muestra la venta para añadir carpetas.

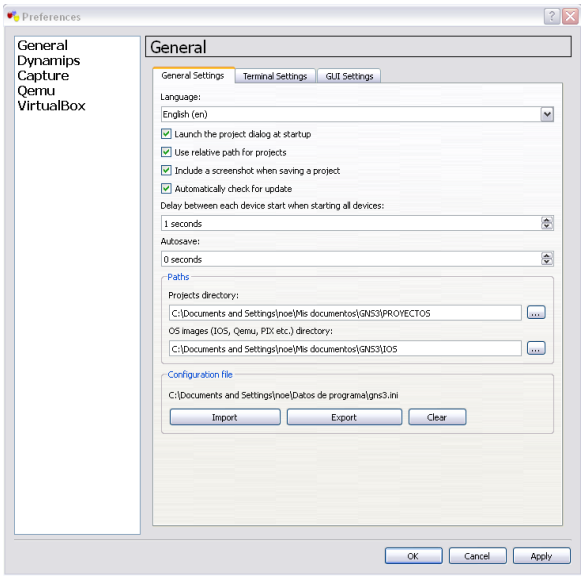

Fig. A.11 Ventana para añadir las carpetas proyectos e IOS.

13. Paso: En la fig. A12 muestra la ventana “Preferences”, se escoge Dynamips y luego seleccionar test setting, lo cual nos permitirá emular los IOS de CISCO. Se enviará un anuncio color verde si es exitoso el test. El test se realiza para conocer si GNS3 puede emular los IOS de CISCO de los equipos cargados.

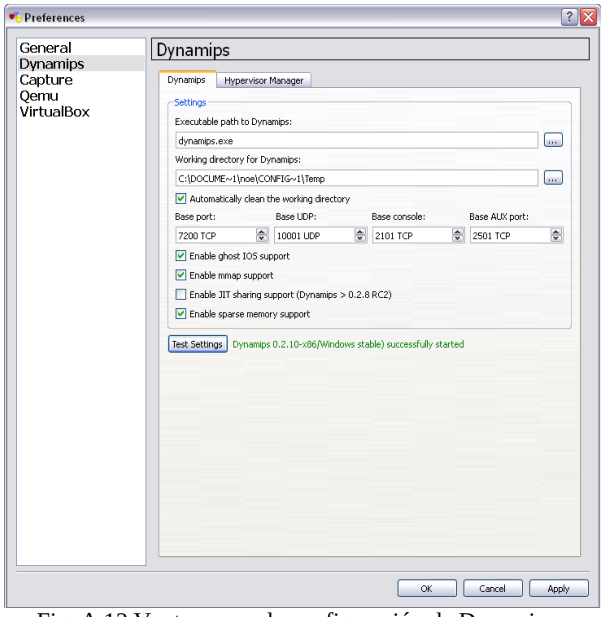

Fig. A.12 Ventana para la configuración de Dynamips.

14. Paso: La tercera casilla de la fig. A.13 se utiliza para añadir las imágenes que utilizaremos, aquí colocaremos la ruta de dónde se encuentra guardada la imagen de IOS del routers 7200 que se utilizará, al final damos guardar.

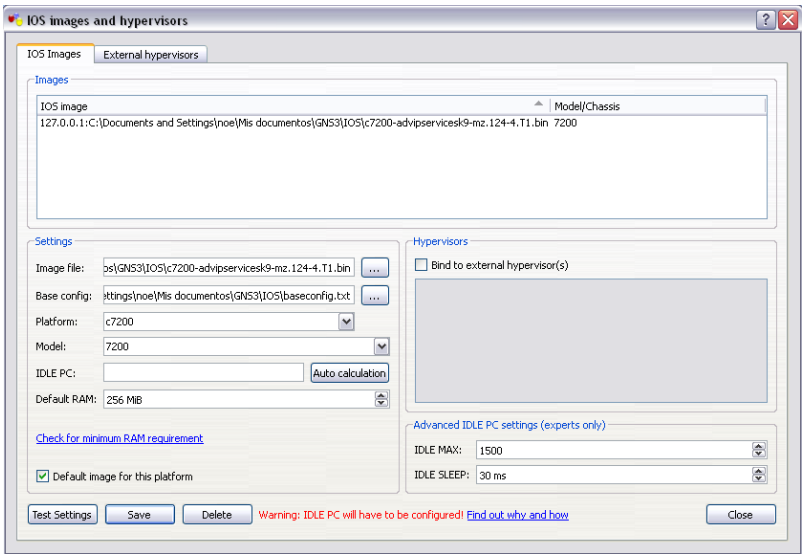

Fig. A.13 Ventana que muestra el IOS imágenes de GNS3 para ejecutar los IOS.

15. Paso: En la ventana principal de GNS3 seleccionar la opción *EDIT*, después seleccionar la opción *preferences,* se abrirá una ventana en la cual seleccionará la opción *QEMU*, como se muestra en la fig. A.14 y por último

seleccionar la opción de *Qemu Guest*, aquí será donde añadirá la aplicación de Qemu para poder emular imágenes de LINUX. Qemu se descarga del siguiente enlace http://www.gns3.net/appliances/, el Qemu descargado es el *Linux Microcore 3.8.2*.

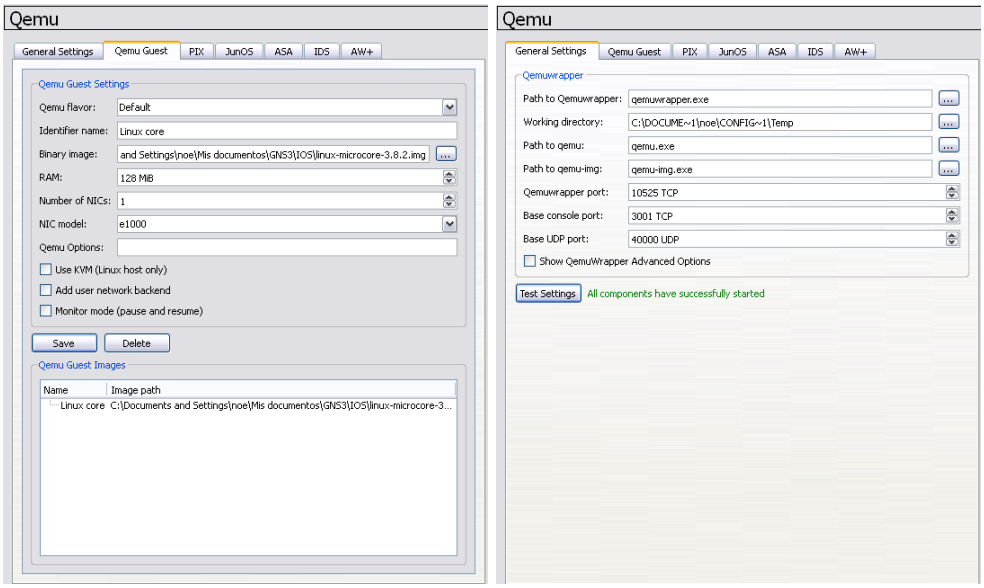

Fig. A.14 Ventana para añadir Qemu para la emulación de Linux.

Para la configuración de Qemu, en la casilla de Identifier name colocamos *Linux core*, en seguida agregamos la ruta de la imagen de Qemu, en la casilla RAM: 128 Mb, en la casilla de Number of NICs colocar 1 y después se guardan los cambios realizados, ahora se selecciona la opción General Setting, enseguida seleccionar *test Setting* para que GNS3 permita emular los Qemu saldrá una leyenda la cual nos anuncia que se pueden utilizar los Qemu correctamente.

16. PASO: finalmente se puede verificar si GNS3 trabaja correctamente realizando la topología de la fig. A.15, se deben configurar cada uno de los dispositivos para su correcto funcionamiento.

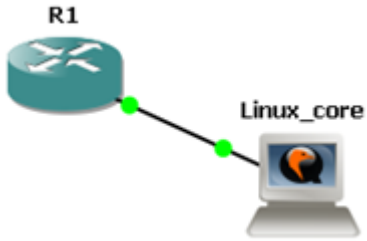

Fig. A.15 ventana que muestra la topología para nuestro ejemplo.

En la fig. A.16 se muestra el ping realizado del router 1 hacia el host, el ping enviado es exitoso.

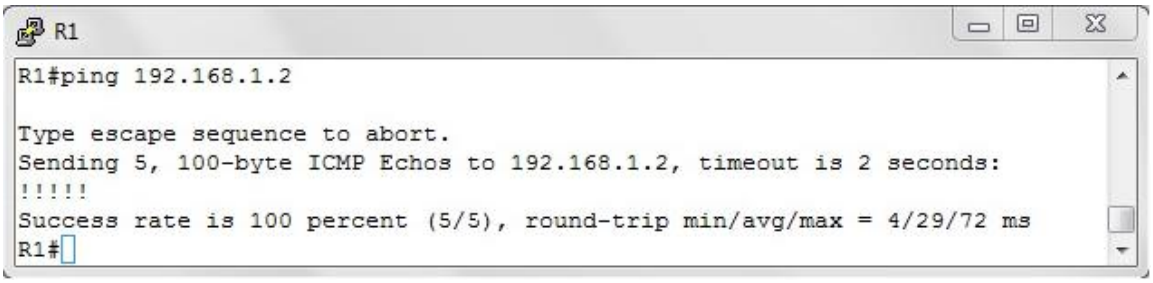

Fig. A.16 figura que muestra el envió del ping realizado del router al host el cual fue exitoso.

En la fig. A.17 muestra el ping realizado del host hacia el router 1, el ping enviado es exitoso por lo que se comprueba la comunicación en ambos equipos.

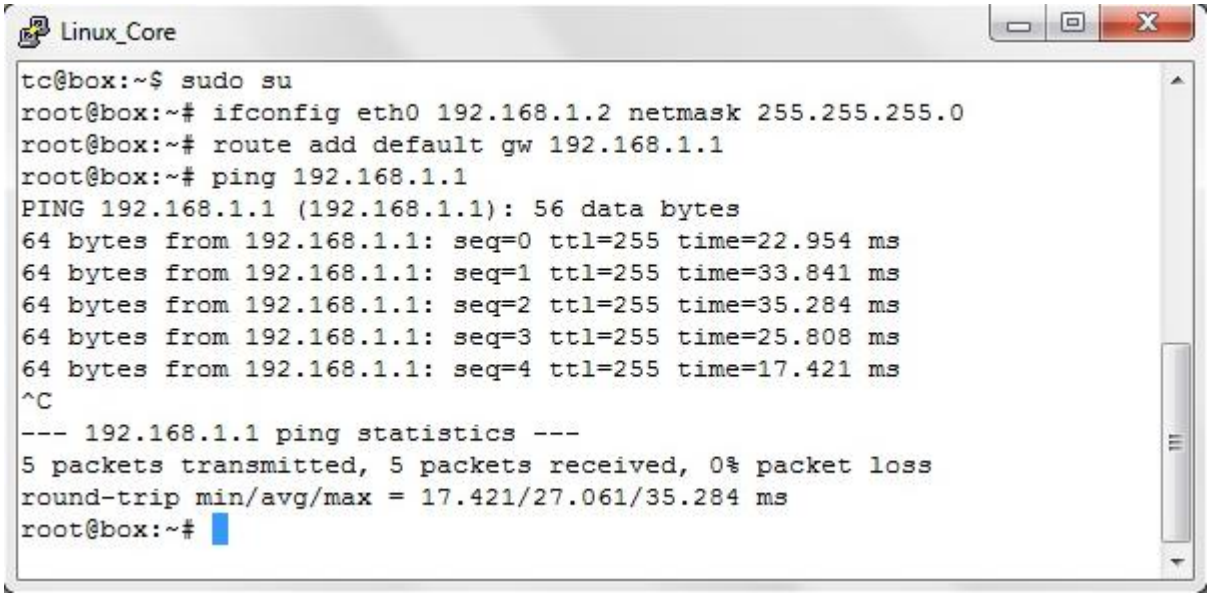

Fig. A.17 figura que muestra la realización del envió del ping realizado del host hacia el router el cual fue exitoso.

APÉNDICE B
Direcciones IP

B.1 Introducción

La dirección IP es una dirección de red lógica que identifica a una computadora para poder comunicarse con otros dispositivos, esta dirección debe ser configurada por un administrador de red o por un servidor que se encarga de proporcionar las direcciones. Las direcciones IPv4 proporcionan más de 4000 millones de direcciones, estas direcciones se componen de dos partes, la parte de red y la parte del host, pero si se realiza una división (subneteo) se tienen tres partes red, subred y host. Para crear subredes deben tomarse en cuenta la cantidad de subredes a crear, la cantidad de host a utilizar y los que se agregarían en un futuro. [100]

B.2 Direcciones IP

Para poder transmitir datos de una computadora a otra y así establecer una comunicación entre ambas se utiliza una dirección única la cual se conoce como dirección de Internet o más comúnmente conocida como dirección IP, el organismo encargado de asignar las direcciones IP es ICANN (*Internet Corporation for Assigned Names an Numbers*, Corporación de Internet para la Asignación de Nombres y Numeración).

Existen dos versiones de direcciones IP: versión 4 (IPv4) y la versión 6 (IPv6). La versión IPv6 no se explicará solo la versión IPv4.

Las direcciones IPv4 están formadas por 32 bits los cuales están divididos en 4 grupos de octetos (8 bytes), la dirección IP se compone de dos partes, un número identificador de red y un número identificador de host, como se muestra en la fig. B.1.

[100] [101]

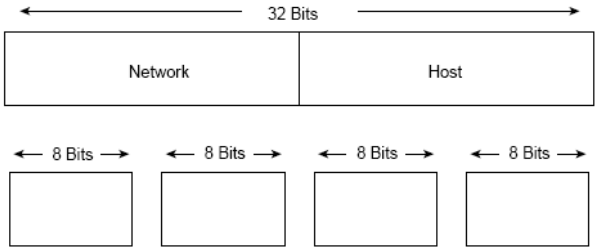

Fig. B.1 Formato de direcciones IPv4 clase B.

Las direcciones IP se representan en formato decimal denominada "*notación de punto decimal*" utilizando el punto para separar cada uno de los octetos, ver fig. B.2.

Binario		Notación punto decimal
11000000 10101000 01100100 00011001	=	192.168.100.25

Fig. B.2 Ejemplo de la Notación punto Decimal.

Las direcciones IPv4 están organizadas en cinco clases: A, B, C, D, E, los primeros 4 bits del primer octeto determinan la clase de una dirección, el resto de los bits se utilizan para identificar a la red y para identificar la parte del host, en la fig. B.3 se muestra el formato de las cinco clases de direcciones.

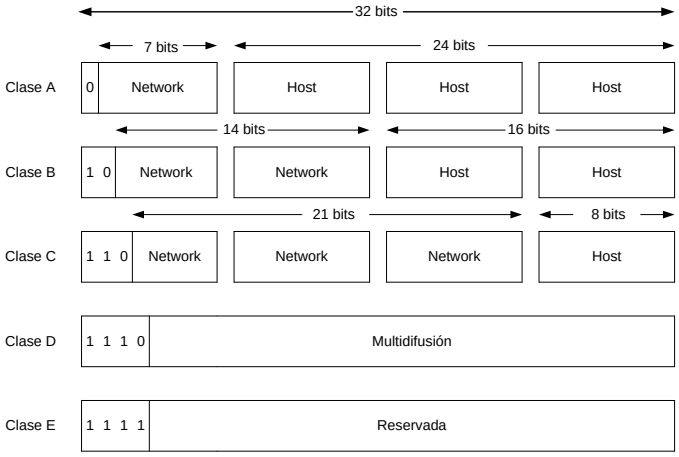

Fig. B.3 Formato de clases de direcciones IP.

- ✓ Clase A: utiliza los bits del 1 al 7 para identificar la red y los bits del 8 al 31 para identificar el host.
- ✓ Clase B: utiliza los bits del 2 al 15 para identificar la red y los bits del 16 al 31 para identificar el host.

- ✓ Clase C: utiliza los bits del 3 al 23 para identificar la red y los bits del 24 al 31 para identificar el host.

En la tabla B.1 muestra el intervalo de direcciones, el número de red y el número de host de cada una de las clases.

Clase	Intervalo de Dirección	Número de redes	Número de host
Clase A	1.0.0.0 – 126.0.0.0	128	16,777,214
Clase B	128.0.0.0 – 191.255.0.0	16384	65534
Clase C	192.0.0.0 – 223.255.255.0	2,097,152	254
Clase D	224.0.0.0 – 239.255.255.254	Direcciones de multidifusión	------
Clase E	240.0.0.0 – 254.255.255.255	Reservada	------

Tabla B.1 Intervalo de direcciones IP

B.3 Subneteo

El RFC 950 propone un procedimiento llamado enmascaramiento de subredes (Subnet Mask) para dividir las direcciones IP, este procedimiento se utiliza para incrementar el número de redes, este procedimiento se basa en usar bits de la parte del host para aumentar el número de redes. [102]

Características:

- ✓ Se reduce el tráfico en las redes.
- ✓ Se tiene una gestión simplificada de la red.
- ✓ Facilidad para identificar y aislar problemas.

Para realizar subredes o llevar a cabo el subneteo se utiliza la máscara de subred el cual es un valor que está formado por 32 bits que identifica que bits de una dirección representan los bits de red y los bits de host, en la fig. B.4 se muestra la parte de red la parte de subred y los host. [103] [104] [105]

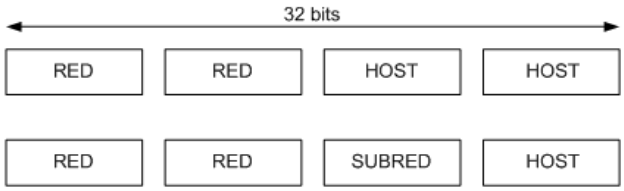

Fig. B.4 Bits tomados de la parte del host.

La máscara de subred utiliza “1” para representar la parte de la red, los “0” se utilizan para determinar la parte del host. Las máscaras de subred también se pueden representar en formato decimal “*notación de punto decimal”*, como se presenta en la fig. B.5.

Clase	Formato	Máscara predeterminada en binario	Máscara predeterminada en decimal
Clase A	Net.Host.Host.Host	11111111 00000000 00000000 00000000	255.0.0.0
Clase B	Net.Net.Host.Host	11111111 11111111 00000000 00000000	255.255.0.0
Clase C	Net.Net.Net.Host	11111111 11111111 11111111 00000000	255.255.255.0

Fig. B.5 Máscaras de subredes predeterminadas.

Otra forma de representar la máscara de subred es utilizando un prefijo (un prefijo es una barra inclinada ***/***) y el valor numérico que es la suma de los bits que representan a la red.

- ✓ Máscara predeterminada clase A ***/*** 8bits
- ✓ Máscara predeterminada clase B ***/*** 16bits
- ✓ Máscara predeterminada clase C ***/*** 24bits

Para crear subredes se utilizan las siguientes ecuaciones:

Para conocer el número de subredes que se pueden usar, se usa dos elevado a la potencia del número de bits asignados a la subred menos dos, la razón de restar dos es por las direcciones de red y la dirección de broadcast, ecuación B.1.

$$2^{x} - 2 = numero\ de\ subredes$$
$$x \rightarrow bits\ prestados\ (1's) \qquad \text{(B.1)}$$

Para conocer el número de host que utilizan para cada una de las subredes, se usa dos elevado a la potencia de los bits restantes (bits en ceros) menos dos, la razón de restar dos es por el identificador de subred y el broadcast de la subred, ecuación B.2.

$$2^{x} - 2 = numero\ de\ subredes$$
$$x \rightarrow bits\ sobrantes\ (0's) \qquad \text{(B.2)}$$

Para conocer las subredes válidas se utiliza la ecuación B.3.

$$256 - mascara\ de\ subred = numero\ base \qquad \text{(B.3)}$$

A. Subneteo de direcciones clase C:

En una dirección clase C sólo dispone de 8 bits para los host, los cuales se ponen a 1 para formar las subredes, estos se van tomando de izquierda a derecha por lo que las máscaras de subred son las que se muestran en la fig. B.6:

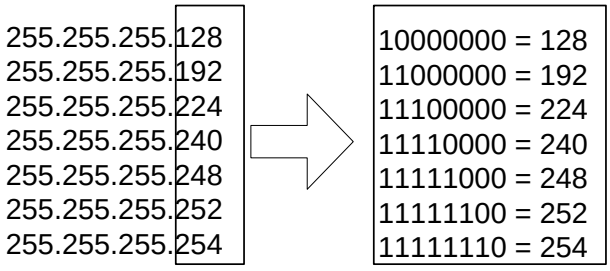

Fig. B.6 Máscaras de subred de clase C.

Las subredes 128 y 254 no se pueden tomar ya que no se pueden crear subredes con solo un bit, se necesitan dos bits para definir los host. Para la máscara de subred **255.255.255.192** la cual toma dos bits del host se tienen dos redes, cada una con 62 host, las subredes validas son 64 y 128, la fig. B.7 muestra las subredes clase C.

Número de Bits	Máscara de subred	Número de subredes	Número de Host
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Fig. B.7 Subredes de clase C, con el número de subredes creadas y el número de host disponibles. [105]

B. Subneteo de direcciones clase B

En las direcciones clase B solo se disponen de dos octetos (16 bits) para los host, los cuales se ponen a 1 al igual que los de clase C para formar las subredes, de estos 16 bits sólo se utilizan 14 bits para subredes y los otros 2 bits para definir los host, las máscaras de subred son las mostradas en la fig. B.8.

255.255.128.0
255.255.192.0
255.255.224.0
255.255.240.0
255.255.248.0
255.255.252.0
255.255.254.0
255.255.255.0
255.255.255.128
255.255.255.192
255.255.255.224
255.255.255.240
255.255.255.248
255.255.255.252

Fig. B.8 Máscaras de subred de clase B.

En la fig. B.9 se puede observar que tenemos más subredes de clase B que las creadas en la clase C.

Número de Bits	Máscara de subred	Número de subredes	Número de Host
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

Fig. B.9 Subredes de clase B.

C. Subneteo de direcciones clase A

Las direcciones de clase A sólo tienen 24 bits tres octetos para los host, los cuales se ponen a 1 al igual que los de clase C para formar las subredes, de estos 24 bits sólo se utilizan 22 bits para subredes, las máscaras de subred son las mostradas en la fig. B.10.

255.128.0.0
255.192.0.0
255.224.0.0
255.240.0.0
255.248.0.0
255.252.0.0
255.254.0.0
255.255.0.0
255.255.128.0
255.255.192.0
255.255.224.0
255.255.240.0
255.255.248.0
255.255.252.0
255.255.254.0
255.255.255.0
255.255.255.128
255.255.255.192
255.255.255.224
255.255.255.240
255.255.255.248
255.255.255.252

Fig. B.10 Máscaras de subred de clase A.

En la fig. B.11 se muestra el número de bits utilizados por cada subred de clase A, la máscara de subred, el número de subredes creadas y el número de host utilizado por cada subred de clase A.

Al trabajar con subredes las direcciones de red se forman poniendo todos los bits de host a cero (0), la dirección de broadcast se forma poniendo todos los bits del host a uno (1) de las direcciones IP, mientras que para formar la máscara de subred todos los bits de red o subred se ponen a uno (1) y los demás bits a cero (0).

Número de Bits	Máscara de subred	Número de subredes	Número de Host
2	255.192.0.0	2	4194302
3	255.224.0.0	6	2097150
4	255.240.0.0	14	1048574
5	255.248.0.0	30	524286
6	255.252.0.0	62	262142
7	255.254.0.0	126	131070
8	255.255.0.0	254	65534
9	255.255.128.0	510	32766
10	255.255.192.0	1022	16382
11	255.255.224.0	2046	8190
12	255.255.240.0	4094	4094
13	255.255.248.0	8190	2046
14	255.255.252.0	16382	1022
15	255.255.254.0	32766	510
16	255.255.255.0	65534	254
17	255.255.255.128	131070	126
18	255.255.255.192	262142	62
19	255.255.255.224	524286	30
20	255.255.255.240	1048574	14
21	255.255.255.248	2097150	6
22	255.255.255.252	4194302	2

Fig. B.11 Subredes de clase A, en la que se aprecia que las subredes de clase A contienen a las subredes de clase B y C.

APÉNDICE C

Equipo de Backbone

En el presente apéndice se muestran las características de los equipos de comunicación utilizados por el backbone de la red CUDI que se encuentran localizados en México D.F., Guadalajara, Monterrey, Tijuana, Cd. Juárez y Cancún.

C.1 Router Cisco 7200 y 7206

El router 7200 es utilizado en redes MAN y WAN, este equipo soporta protocolos IP, calidad del servicio QoS, soporta VPNs, protocolos VOIP (H.323, SIP), soporta protocolos de enrutamiento tanto estáticos como dinámicos, además cuenta con slots para diferentes tarjetas con las que es compatible, las versiones del software soportadas para el router 7200 son: 12.1(5)E, 12.1(5)T, 12.2, 12.4 y las versiones soportadas por el router 7206 son: 12.0(5)S, 12.1(1)T, 12.1(1)XE, 12.1(1), en la fig. C.1 se muestra la imagen y en la tabla C.1 sus características.

Fig. C.1 Router cisco 7200 (Familia de 7200 se encuentra en el ANL (Laboratorio de Redes Avanzadas)). [105] [106]

Características		
Router	7200	7206
Procesador	RM7000A 262Mhz	RM5271 200Mhz
SDRAM	128 – 256 Mb	128 – 256 Mb
Flash	16Mb	48- 128Mb
NVRAM	512Kb	512Kb
Velocidades	T1, E1, SONET, ATM,	E1, sonet, OC-3, ATM, T1, T3, E3
Puertos	Fast Ethernet,, ATM (T3, OC-3), HSSI, seriales, T3, paralelos	Ethernet, Fast Ethernet, FDDI, serials, FDX, HDX
Alimentación	100-240 VAC 50/60Hz	100-240 VAC 50/60Hz
Fuente de voltaje	-24 a -60 VDC	-24 a -60 VDC

Tabla C.1 Características Serie 7200 y 7206. [105] [106]

C.2 Router Cisco 7513

El router cisco 7513 pertenece a la serie 7500 a nivel backbone soporta protocolos a nivel de capa 2 y capa 3 como son: ARP, ICMP, IP, IP sobre ATM, TCP, telnet, FTP, UDP, Frame Relay, IPX, Apple Talk, VLAN, IPV6, ATM, PPP, los protocolos de enrutamiento que maneja son los siguientes: EIGRP, IGRP, IS-IS, OSPF, BGP, PIM y RIP, en cuanto a la seguridad y gestión de redes maneja RADIUS, SNMP, FTP, AAA, CHAP, PAP y TACACs, las versiones del software IOS (Internetworking Operating System) soportadas son: 10.3, 11.1(8), 12.0, 12,1, en la fig. C.2 se muestra la imagen y en la tabla C.2 se presentan sus características. [107][108]

Fig. C.2 Router cisco 7513. [107]

Características	
Procesador	RSP(Router Switch Processor)16, RSP8, RSP4,RSP2
Flash	16Mbps, 8Mbps
Velocidades	DS0, DS1, DS3, STM-1, SONET, T3/E3, T1/E1/T3, ATM, OC-3
Puertos	Fast Ethernet, Gigabit Ethernet, FDDI (FDX,HDX), ATM, SONET OC3, Seriales, Token Ring, T1, T3
Alimentación	16A 100VCA, 7A 240VCA
Fuente de voltaje	-48 a -60 CC

Tabla C.2 Características del router 7513. [107] [108]

C.3 Router Cisco 7606

El router 7606 es un dispositivo capaz de soportar múltiples aplicaciones a nivel WAN protocolos IP, triple-play (voz, vídeo y datos), se pueden seleccionar tarjetas para diversas aplicaciones como los módulos Flex Wan (adaptadores DS-0 a OC-3, ATM, puertos Ethernet y Fast Ethernet), módulos Ethernet y Gigabit Ethernet, módulos de servicios para seguridad (Firewall), cuenta con ranuras para procesadores redundantes y fuentes de alimentación redundantes, las versiones de IOS soportadas son 12.1 como mínimo, en la fig. C.3 se muestra la imagen y en la tabla C.3 se presentan sus características. [109 [110]

Fig. C.3 Router cisco 7606. [109]

Características	
Procesador	SPA (Shared port adaptors)-200, SIP (SPA interface processors)-400
NVRAM	512kb
Velocidades	OC-3/STM-1, OC-12/STM4, OC-48/STM-16 paquetes sobre sonet, OC-192/STM-62 PoS, OC-3/STM-1 ATM, OC-12/STM-4 ATM y OC-48/STM-16 ATM
Puertos	Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet
Alimentación	1900W AC, 2700W AC
Fuente de voltaje	1900W CC, 2700W CC

Tabla C.3 Características del router 7606. [109] [110]

C.4 Router GSR (Gigabit Switch Router) 10000

Es un router a nivel de backbone el cual soporta aplicaciones triple play, es utilizado para migrar de ATM a Gigabit Ethernet, soporta múltiples servicios IP, ofrece QoS, ofrece L2TP para la realización de túneles, cuenta con redundancia tanto para el procesador como para las fuentes de alimentación, la versión de IOS soportada es 12.2 como mínimo, en la fig. C.4 se muestra la imagen y en la tabla C.4 se presentan sus características. [111] [112]

Fig. C.4 Router cisco 10000. [111]

Características	
Procesador	10000-SIP-600 800MHz
Velocidades	ATM, Frame Relay, E1, STM-1, OC-3, OC-12, E3
Puertos	Gigabit Ethernet, Fast Ethernet, OC, ATM,
Alimentación	100-240 VCA 50/60 Hz
Fuente de voltaje	-48/-60 VDC

Tabla C.4 Características del router 10000. [111] [112]

APÉNDICE D

Comandos de Configuración

En el presente apéndice se presentan los comandos de configuración utilizados por los routers, durante la simulación y la emulación de la red CUDI por medio del Protocolo OSPF, como se muestran en las tablas D.1 y D.2. [113]

Comando de CLI IOS de CISCO	Descripción
Router1>	Modo usuario
Router1>**enable**	Accede al modo privilegiado
Router1#	Modo privilegiado.
Router1#**configure terminal**	Cambio del modo privilegiado a modo de configuración global.
Router1(config)#	Modo configuración global.
Router1(config)#**hostname CICESE**	*Hostname* para cambiar el nombre del router.
CICESE(config)#**interface serial 1/0**	*Interface* comando utilizado para modificar la configuración de la interfaz.
CICESE(config-if)#**ip address 172.10.1.1 255.255.0.0**	*ip address* utilizado para asignar una dirección IP a la interfaz.
CICESE(config-if)#**clock rate 56000**	*Clock rate* utilizado para cambiar la velocidad del reloj en una interfaz serie.
CICESE(config-if)#**no shutdown**	Habilita la interfaz
CICESE(config)#**router ospf 1**	*router* comando utilizado para asignar el tipo de enrutamiento.
CICESE(config-router)#**network 172.10.0.0 0.0.255.255 area 0**	*Network* habilita OSPF en todas las interfaces que pertenezcan a esa red.

Tabla D.1 Comandos utilizados para la configuración de OSPF del router CICESE.

Comando de CLI IOS de CISCO	Descripción
CICESE(config)#**interface serial s1/0**	*Interface* comando utilizado para modificar la configuración de la interfaz.
CICESE(config-1f)#**bandwidth 34000**	Realiza cambios en el ancho de banda, y se calcula el costo del enlace.
CICESE(config-if)#**ip ospf cost 2**	Realiza cambios en el costo de un enlace.

Tabla D.2 Comandos utilizados para la configuración del costo.

El comando CICESE(config-router)#**network** *address wildcard mask* **area** *area id*, utiliza una máscara wildcard la cual es el inverso de la máscara de red, por ejemplo si se tiene la siguiente dirección IP 172.10.0.0/16 su máscara de red es 255.255.0.0 mientras la máscara wildcard es 0.0.255.255, el comando network utiliza esta máscara wildcard para determinar cómo leer la dirección de red. En las tablas D.3 y D.4 se muestran otros comandos de configuración para OSPF. [114] [115]

Comando de CLI IOS de CISCO	Descripción
Router(config-router)#**logadjacency-changes detail**	Configura el router para enviar un mensaje cuando hay un cambio de estado entre vecinos OSPF.
Router(config)#**interface loopback** 0	Crea una interfaz virtual denominada loopback 0, y
Router(config-router)#**router-id** 10.1.1.1	Establece el ID de router a 10.1.1.1. El cual se carga nuevamente cuando se reinicia el proceso de OSP.
Router(config-router)#**no router-id** 10.1.1.1	Elimina el ID del router.
Router(config-if)#**ip ospf priority** valor	Cambia el valor de la prioridad de la interfaz. El valor puede estar entre 0 y 2555, con un valor de 0 el router no se elige como DR.

Tabla D.3 Otros Comandos utilizados en la configuración de OSPF.

Comando de CLI IOS de CISCO	Descripción
Router(config-router)#**area 0 authentication**	Permite la autenticación y los datos serán enviados sin cifrar.
Router(config-if)#**ip ospf authentication-key** nombre	Establece una clave (contraseña) para un *nombre*. La contraseña puede ser cualquier cadena de caracteres de 8 bytes de longitud.
Router(config-if)#**ip ospf hellointerval timer** valor	Cambia el tiempo de envió de los paquetes HELLO en segundos.
Router(config-if)#**ip ospf deadinterval** valor	Cambia el intervalo de tiempo, en (segundos).
Router#**clear ip route ***	Borra toda la tabla de enrutamiento y la reconstruye nuevamente.
Router#**clear ip route a.b.c.d**	Borra rutas especificas a a.b.c.d de red
Router#**clear ip opsf counters**	Restablece los contadores de OSPF.
Router#**clear ip ospf process**	Restablece el proceso de OSPF y vuelve a crear a los vecinos, la base de datos y la tabla de enrutamiento.
ter#**debug ip ospf events**	Muestra los eventos de OSPF
Router#**debug ip ospf adjacency**	Muestra los estados de OSPF, muestra la elección del DR/BDR entre los routers adyacentes.
Router#**debug ip ospf packets**	Muestra paquetes OSPF

Tabla D.4 Otros Comandos utilizados en la configuración de OSPF. [113]

APÉNDICE E

Velocidades de transmisión

En el presente apéndice se presentan las velocidades de transmisión utilizadas en redes de datos, la tabla E.1, E.2 se muestran las velocidades y sus equivalencias. [116]

Nombre de la Señal Digital (DS)	Velocidad	Número de DS0s utilizado	Nombre equivalente de T-carrier	Nombre equivalente E-carrier
DS0	64kbps	1	-	--
DS1	1.544Mbps	24	T1	--
--	2.048Mbps	32	--	E1
DS1C	3.152 Mbps	48	--	--
DS2	6.312 Mbps	96	T2	--
--	8.448 Mbps	128	--	E2
--	34.368 Mbps	512	--	E3
DS3	44.736 Mbps	672 o 28 DS1s	T3	--
--	139.264 Mbps	2048	--	E4
DS4/NA	139.264 Mbps	2176	--	--
DS4	274.176 Mbps	4032	--	--
-	565.148 Mbps	4 E-4 canales	--	E5

Tabla E.1 Equivalencias de las velocidades de transmisión. [115]

Señal SONET	Velocidad	Señal SDH	Capacidad SONET	Capacidad SDH
OC-1 (STS-1)	51.84 Mbps	STM-0	28 DS-1s o 1 DS-3	21 E1s
OC-3 (STS-3)	155.42 Mbps	STM-1	84 DS-1s o 3 DS-3s	63 E1s o 1E4
OC-12 (STS-12)	622.08 Mbps	STM-4	336 DS-1s o 12 DS-3s	252 E1s o 4 E4s
OC-48 (STS-48)	2.488 Gbps	STM-16	1344 DS-1s o 48 DS-3s	1008 E1s o 16 E4s
OC-192 (STS-192)	10 Gbps	STM-64	5376 DS-1s o 192 DS-3s	4032 E1s o 64 E4s
OC-256	13.271 Gbps			
OC-768	40 Gbps			

Tabla E.2 Equivalencias de las velocidades de transmisión. [116]

STS-1 es equivalente a OC-1

STC-1 = OC1 = 51.84Mbps

STC-3 = OC3 = STM-1 = 155Mbps

STC-9 = OC9 = STM-3 = 9 (no usado)

STC-12 = OC312 = STM-4 = 622Mbps

STC-18 = OC18 = STM-6 = 18 (no usado)

STC-24 = OC24 = STM-8 = 24 (no usado)

STC-36 = OC36 = STM-12 = 36 (no usado)

STC-48 = OC48 = STM-16 = 2.5Gbps

E1 = 32 64-kbps canales = 2.048Mbps

E0 = 64kbps

4 * E1 = E2

4 * E2 = E3

E3 = 34Mbps

STM = Syncronous Transport Module (ITU-T)

STS = Synchronous Transfer Signal (ANSI)

OC = Optical Carrier (ANSI)

SDH = Synchronous Digital Hierarchy

Un SDH STM-1 tiene la misma velocidad de bits que el STS-3 SONET, pero las dos señales de contienen diferentes estructuras de trama.

REFERENCIAS

Se utiliza el estándar ISO 690-2 para citar las fuentes de información de internet para dar formalidad a las fuentes consultadas.

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

[2] Robert Kahn, Demostration at International Computer Communications Conference, *Request for comments: 371, BBN*, 12 July 1972.

[3] Steve Crocker, Host Software, *Request for comments: 1, Network Working Group*, UCLA, 7 April 1969.

[4] José Ignacio Castillo Velázquez, *Redes de Datos: contexto y evolución*, Edit. SAMSARA, 2014, pag 36, 37.

[5] ARPANET, ARPANET mapa, [en línea], 2014, [Última visita: 24 de enero de 2014] Disponible: http://som.csudh.edu/fac/lpress/history/arpamaps/ .

[6] José Ignacio Castillo, *Internet y la WEB no son lo mismo: día internacional de Internet 2011*, Latin America and the Caribbean, volumen 22, number 3, June 2011-2013

[7] Internetsociety, IPV6, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internetsociety.org/history-timeline/world-ipv6-launch

[8] José Ignacio Castillo Velázquez, *Redes de Datos: contexto y evolución*, Edit. SAMSARA, 2014, Capitulo II.

[9] José Ignacio Castillo, *Introducción a las tecnologías de red: una vista general y el modelo OSI*, UACM-SLT, 2010-2013.

[10] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/

[11] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/search/?cx=005837499705399601518%3Amioyfjwg54i&cof=FORID%3A10&ie=UTF-8&q=history&sa=Search

[12] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/presentations/981027-BT.../981027-BT-Ann.ppt

[13] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/presentations/.../20031013-Internet2101-Almes.ppt

[14] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/internet-2/architecture.html

[15] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/presentations/.../Luker's%20Presentation.ppt

[16] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/.../20061206-observatory- summerhillCashmanZekauskasBoyd.ppt

[17] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/presentations/spring04/20040421-Abilene-Corbato.pdf

[18] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/communities-groups/members/

[19] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/products-services/advanced-networking/layer-3-services/

[20] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://noc.net.internet2.edu/

[21] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/presentations/97-06-Denver.../970612-Guy.htm

[22] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/presentations/980603.../980603-AAAS-DVH.ppt

[23] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/presentations/i2ovrvw/sld017.htm

[24] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/presentations/981027-BT-Ann/sld074.htm

[25] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: www.internet2.edu/presentations/.../97-06-Denver-Giga-Tech.PPT

[26] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/media/medialibrary/2013/07/31/Internet2-Network-Infrastructure-Topology.pdf

[27] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/media/medialibrary/2013/10/01/I2-Network-Infrastructure-Layer-3.pdf

[28] Red Internet 2, [en línea], 2014, [Última visita: 9 de enero de 2014] Disponible: http://www.internet2.edu/communities-groups/members/

[29] Red CANARIE, [en línea], 2014, [Última visita: 20 de enero de 2014] Disponible: http://www.canarie.ca/

[30] Red DANTE, [en línea], 2014, [Última visita: 16 de enero de 2014] Disponible: http://www.dante.net/Pages/default.aspx

[31] Red APAN, [en línea], 2014, [Última visita: 20 de enero de 2014] Disponible: http://www.apan.net/

[32] Red GEANT, [en línea], 2014, [Última visita: 16 de enero de 2014] Disponible: http://www.geant.net/Pages/default.aspx

[33] Red Internet 2, [en línea], 2014, [Última visita: 15 de enero de 2014] Disponible: www.internet2.edu/presentations/.../20050215-CLARA-Porto.ppt

[34] Red CLARA, mapa [en línea], 2014, [Última visita: 15 de enero de 2014] Disponible: http://www.redclara.net/index.php?option=com_content&view=article&id=51&Itemid=347&lang=es

[35] Red CAREN, [en línea], 2014, [Última visita: 18 de enero de 2014] Disponible: http://caren.dante.net/Pages/home.aspx

[36] Red ORIENTOLUS, [en línea], 2014, [Última visita: 19 de enero de 2014] Disponible: http://www.orientplus.eu/

[37] Red AFRICACONNECT, [en línea], 2014, [Última visita: 18 de enero de 2014] Disponible: http://www.africaconnect.eu/pages/home.aspx

[38] Red EUMEDCONNECT, [en línea], 2014, [Última visita: 18 de enero de 2014] Disponible: http://www.eumedconnect3.net/Pages/home.aspx

[39] Red CARIBNET, [en línea], 2014, [Última visita: 19 de enero de 2014] Disponible: http://www.ckln.org/home/

[40] Red DANTE, [en línea], 2014, [Última visita: 20 de enero de 2014] Disponible: http://www.dante.net/DANTE_Network_Projects/Pages/default.aspx

[41] Red GEANT, [en línea], 2014, [Última visita: 20 de enero de 2014] Disponible: http://www.geant.net/Network/Global-Connectivity/Pages/World_Regions-Asia_Pacific.aspx

[42] Red CUDI, [en línea], 2013, [Última visita: 23 de enero de 2014] Disponible: http://www.cudi.edu.mx

[43] Red CUDI, Misión, [en línea], 2013, [Última visita: 18 de diciembre de 2013] Disponible: http://www.cudi.mx/acerca-de-cudi/mision-vision

[44] Red CUDI, Antecedentes, [en línea], 2013, [Última visita: 18 de diciembre de 2013] Disponible: http://www.cudi.mx/acerca-de-cudi/antecedentes

[45] Red CUDI, Miembros de CUDI, [en línea], 2013, [Última visita: 20 de diciembre de 2013] Disponible: http://www.cudi.mx/acerca-de-cudi/lista-miembros

[46] Red CUDI, Instituciones conectadas, [en línea], 2013, [Última visita: 20 de diciembre de 2013] Disponible: http://www.cudi.mx/conexion/instituciones-conectadas

[47] Red CUDI, Presentaciones, [en línea], 2014, [Última visita: 20 de enero de 2014] Disponible: http://www.cudi.mx/acervos/presentaciones

[48] Red CUDI, Conexión a la red CUDI, [en línea], 2014, [Última visita: 24 de enero de 2014] Disponible: http://www.cudi.mx/conexion

[49] Red CUDI, Topología de la red, [en línea], 2014, [Última visita: 24 de enero de 2014] Disponible: http://www.cudi.mx/conexion/backbone

[50] Red CUDI, Alternativas de conexión, [en línea], 2014, [Última visita: 24 de enero de 2014] Disponible: http://www.cudi.mx/conexion/alternativas-conexion

[51] Red CUDI, Red NIBA, [en línea], 2014, [Última visita: 24 de enero de 2014] Disponible: http://www.cudi.mx/conexion/red-niba

[52] Red CUDI, NOC CUDI, [en línea], 2014, [Última visita: 24 de enero de 2014] Disponible: http://www.cudi.mx/noc-cudi

[53]Catherine Paquet, Diane Teare, *Creación de Redes Cisco Escalables*, Cisco Press,Ed. Pearson, pag 5, 6, 15.

[54] William Stalling, *Comunicaciones y Redes de Computadores*, Ed. Pearson, Prentice Hall, pag 397-400.

[55] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 204-207.

[56] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag 77-78.

[57] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 208.

[58] D.L. Mills, *Request for comments: 904*, *Network Working Group*, April 1984.

[59] K. Lougheed, Y Rekhter, *Request for comments: 1105*, *Network Working Group*, Cisco Systems, IBM Corp, June 1989.

[60] Y. Rekhter, *Request for comments: 1771*, *Network Working Group*, Cisco System, T. Li, IBM Corp, March 1995.

[61] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag 80, 81.

[62]Catherine Paquet, Diane Teare, *Creación de Redes Cisco Escalables*, Cisco Press,Ed. Pearson, pag 8-10,15-19.

[63] C. Hedrick, *Request for comments: 1058, Network Working Group*, Rutgerts University, June 1988

[64]Steve Spanier, Tim Stevenson, *Tecnologías de interconectividad de redes*,Cisco System, Ed. Prentice Hall, Capitulo 47.

[65] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag. 109-122.

[66] Todd Lammle, *CCNA: Cisco Certified Network Associate*, Study Guide, Ed. Copyright 200 SYBEX, Inc, Alameda, CA, pag. 301-306.

[67] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 208-211.

[68] G Malkin, *Request for comments: 1723, Network Working Group*, Xylogics, November 1988

[69]Steve Spanier, Tim Stevenson, *Tecnologías de interconectividad de redes*,Cisco System, Ed. Prentice Hall, Capitulo 47.

[70] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag. 137-150.

[71] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 211.

[72] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag. 90, 174, 175.

[73]Steve Spanier, Tim Stevenson, *Tecnologías de interconectividad de redes*,Cisco System, Ed. Prentice Hall, Capitulo 42.

[74] Todd Lammle, *CCNA: Cisco Certified Network Associate*, Study Guide, Ed. Copyright 200 SYBEX, Inc, Alameda, CA, pag. 307-312.

[75] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 2014.

[76]Catherine Paquet, Diane Teare, *Creación de Redes Cisco Escalables*, Cisco Press,Ed. Pearson, pag 229-249.

[77] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag. 173-199.

[78] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 2014.

[79] J. Moy, OSPF, *Request for comments: 1247, Network Working Group*, Proteon INC., July 1991.
[80]Steve Spanier, Tim Stevenson, *Tecnologías de interconectividad de redes*,Cisco System, Ed. Prentice Hall, Capitulo 46.

[81]Catherine Paquet, Diane Teare, *Creación de Redes Cisco Escalables*, Cisco Press,Ed. Pearson, pag 93-134.

[82]Ernesto Ariganello, Enrique Barrientos Sevilla, *Redes CISCO CCNP a Fondo: Guia de studio para profesionales*, Alfaomega Ra-Ma, 2010, pag 97-99.

[83] Thomas M, Thomas II, *OSPF Network Design Solutions*, Cisco Press, 73.

[84]Catherine Paquet, Diane Teare, *Creación de Redes Cisco Escalables*, Cisco Press, Ed. Pearson, pag 100,101.

[85] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson.

[86] CCNA Exploration, *Conceptos y protocolos de enrutamiento*, Guía portátil CISCO, Versión 4.0, Cisco Press, Ed. Pearson, pag. 217-235.

[87] Michael A. Gallo William M. Hancock, *Comunicación entre computadoras y tecnologías de redes*, Ed. Thomson, pag, 212-213.

[88] J Moy, OSPF v2, *Request for comments: 2328, Network Working Group*, Ascend Communications, Inc, April 1998.

[89] R. Coultun, OSPF v3, *Request for comments: 2740, Network Working Group*, Siara Systems, Juniper Networks, Sycamore Networks, December 1999.

[90] R. Callon, IS-IS, *Request for comments: 1195, Network Working Group*, Digital Equipement Corporation., December 1990.

[91] Ernesto Ariganello, Enrique Barrientos Sevilla, *Redes CISCO CCNP a Fondo guía de estudio para profesionaless*, Ed. RA-MA.

[92] Protocolo IS-IS, Protocolo IS-IS, [en línea], 2014, [Última visita: 26 de Marzo de 2014] Disponible:http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml

[93] Philips Smith, *IS-IS tutorial*, Ed. Cisco Press, 2009.

[94] David C. Plummer, ARP, *Request for comments: 826, Network Working Group*, November 1982.

[95] J. Postel, ICMP, *Request for comments: 792, Network Working Group*, ISI, September 1981.

[96] Richard Petersen, *Manual de referencia Linux*, Ed. Mcgraw- hill, segunda edición, 2001, pag. 537-559

[97] José Manuel Huidobro loya, Rafael Conesa Pastor, *Sistemas de telefonía*, quinta edición, Ed. Thomson, 2006, pag, 304-305.

[98] Robert J. Shimonski, Wally Eaton, Umer Khan, Yuri Gordienko, *Snifer Pro: network optimization & Troubleshooting Handbook*, Ed. SynGress, 2002, pag. 2-5.

[99] GNS3, GNS·, [en línea], 2014, [Última visita: 16 de Abril de 2014] Disponible: http://www.gns3.net/

[100] William Stalling, *Comunicaciones y Redes de Computadores*, Ed. Pearson, Prentice Hall.

[101] Andrew S. Tanenbaum, *Redes de computadoras*, Ed. Pearson, Tercera edición.

[102] J. Postel, j.mogul, Subnetting, *Request for comments: 950, Network Working Group*, August 1985.

[103] Steve Spanier, Tim Stevenson, *Tecnologías de interconectividad de redes*, Ed. Prentice Hall.

[104] Todd Lammle, *CCNA: Cisco Certified Network Associate study Guide*, Ed. Corpyright SYBEX, second edition 2000, pag. 100-157.

[105] José Ignacio Castillo, Juan Arnulfo López Ruiz, Simulación de Casos practicos de Subredes clase C en IPV4, Universidad Autónoma de la Ciudad de México, Campus SLT, DF. México.

[105] CISCO, *Data Sheet: Cisco 7200 series router,* 1992.

[106] CISCO, *Data Sheet: Cisco 7206 series routers*, 1992

[107] CISCO, *Data Sheet: Cisco 7500 series routers,* 1992.

[108] CISCO, Router 7513, *Cisco 7500 series installation and configuration guide,* 2005.

[109] CISCO, *Data Sheet: Cisco 7606 router*, 2014.

[110] CISCO, Router 7606, *Cisco 7600 router module installation guide,* 2010.

[111] CISCO, *Data Sheet: Cisco 10000 series routers,* 2007.

[112] CISCO, Router 10000, *Cisco 10000 series router SIP and SAP Hardware installation guide,* 2009.

[113] Scott Empson, *CCNA Portable Command Guide*, Ed. Ciscopress 2008, pag 91, 101.

[114] Ernesto Ariganello, Enrique Barrientos Sevilla, *Redes Cisco CCNP a Fonfo: guía de estudio para profesionales*, Ed. Alfaomega Ra-MA, primera edición 2010, pag 912, 913.

[115] Catherine Paquet, Diane Teare, *Creación de Redes Cisco Escalables*, Cisco Press, Ed. Pearson, pag 116, 117.

[116] Tomas M. Thomas II,*OSPF Network Desing Solutions*, Cisco Press, Ed. Pearson, Second Edition 2003, pag 20.