28

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIO PROFESIONALES
ARAGON

"SISTEMA DE NOMBRES DE DOMINIO EN REDUNAM"

T E S I S

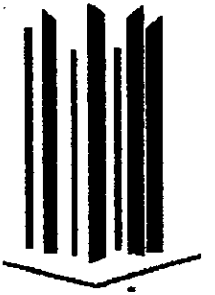
PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

SARAI JEZABEL PEÑALOZA PEREZ

ASESOR:
ING. OCTAVIO HERRERA RUIZ



ARAGON, ESTADO DE MEXICO ~~1999~~ 2000

ARAGON

G R A C I A S:

A mi Papá, Mamá, Andrea, Sergio y Pita

Porque juntos, con nuestro amor, apoyo y comprensión logramos que esta meta que me había fijado en mi vida, llegara a su fin.

A mi chaparro

Porque me haz devuelto la ilusión y la confianza, siendo nuestro amor una motivación y un soporte para seguir adelante en mi camino.

A Rocío, Raquel, Edgar, Eric, Rene, Teck, Vado y Andrés

Que con su amistad incondicional hicieron que mis estudios profesionales fueran una experiencia maravillosa, imposible de olvidar.

A Octavio

Por su valioso asesoramiento en este trabajo de tesis.

Al NIC, en especial a Mariela e Ivette

Por haber hecho que mi estancia en DGSCA fuera una bonita experiencia.

SISTEMA DE NOMBRES DE DOMINIO EN REDUNAM

INTRODUCCIÓN

El Sistema de Nombres de Dominio es un término poco conocido, incluso para aquellos que utilizan Internet frecuentemente, ya sea para buscar alguna información en periódicos, efectuar alguna compra o cualquier otra actividad académica, comercial o de entretenimiento. Sin embargo, este sistema es utilizado en cada momento por casi todos los servicios que emplea un usuario de Internet: el correo, el www, el telnet, etc..

Al hacer uso de cualquiera de los servicios anteriores, el usuario puede percibir la labor que cumple el DNS para que dichos servicios sean amigables para él. En Internet, todas las computadoras solo manejan direcciones numéricas, mejor conocidas como direcciones IP, las cuales no son fáciles de manejar por las personas; como se puede ver si al escoger 10 números telefónicos al azar, es fácil recordarlos?; esto mismo sucedería si se trataran de recordar diez direcciones IP en Internet arbitrariamente; por lo que la labor del DNS consiste en realizar un mapeo entres los nombres y las direcciones IP en Internet. El DNS es un mecanismo estándar utilizado para publicar y tener acceso a toda clase de información sobre cualquier hosts, no necesariamente para conocer su dirección IP.

Otra característica importante del DNS es que garantiza el acceso a la información a través de un sistema distribuído, y no necesariamente se requiere introducir la información a algún sitio central al que periódicamente se tenga que hacer alguna copia de una base de datos maestra. Simplemente debemos asegurarnos cual es nuestro dominio, el que será dado de alta en el servidor de nombres. Este se encargará de que los datos del dominio, estén disponibles para todos los demás servidores de nombres a través de la red.

Debido a que las bases de datos son distribuidas, el sistema tiene la habilidad de localizar cualquier dominio que sea requerido. El DNS brinda a los servidores de nombres la inteligencia de navegar a través de las bases de datos para encontrar datos de cualquier dominio.

Dado que el manejo de los dominios se hace a nivel mundial, el DNS cuenta con algunos puntos críticos que deben tomarse en cuenta para su correcto funcionamiento. Entre estos puntos se encuentra la facilidad de repetir algún dato en cualquiera de los servidores de nombres, lo que se vería reflejado hasta que se llevara a cabo la consulta de los mismos.

Pero el punto mas grave con el DNS es que a pesar de su generalizado uso en Internet, se tiene muy poca información sobre el manejo y administración de éste. Muchos administradores en Internet, han hecho ajustes con la información de sus proveedores, de manera que puedan dar asesorías por medio de listas de correo. La carencia de información sobre este tema, ha ocasionado que no se vea la gran importancia que tiene el DNS en el mundo de Internet.

Pero a pesar de la escasa información, el tema del DNS puede ser abordado desde diversos enfoques (arquitectura cliente-servidor, seguridad, etc.) y cada uno de ellos puede ser ampliamente desarrollado. En este trabajo elegí presentar exclusivamente los elementos mas relevantes para el entendimiento, administración y manejo del DNS. Este enfoque práctico se debió a la necesidad de contar con información que sustentara el desarrollo actual que se tiene de este servicio en la RedUNAM y facilitará la continuidad en la prestación del mismo. Así pues, espero que en lo futuro, mi trabajo sirva para dos fines básicamente: el de introducción y el de documentación.

Con los objetivos mencionados anteriormente, se decidió dividir el trabajo en cuatro capítulos que a continuación describo:

Capítulo 1 - Conceptos Generales: se presentan algunos conceptos del mundo de Internet, su historia, la importancia que ha tenido en México, así como el uso de las direcciones IP y de los nombres de dominio. También se aborda en el tema de TCP/IP para entender lo que es el direccionamiento de la información.

Capítulo 2 - Sistema de Nombres de Dominio (DNS): se describe lo que es en si el Sistema de Nombres de Dominio, su historia, como se encuentra organizado el espacio de nombres de dominio, los dominios en general, y los servidores de nombres, como se lleva a cabo el mapeo, así como también la configuración de cada uno de los archivos de la Base de Datos. Se da una breve explicación de lo que es el BIND como software para el DNS.

Capítulo 3 - Herramientas de Búsqueda: se describe el manejo del Nslookup como una herramienta poderosa para llevar a cabo consultas en el DNS; así como técnicas para consultar a servidores de nombres remotos.

Capítulo 4 - El sistema de Nombres de Dominio (DNS) en RedUNAM: se presentan las características de cada uno de los servidores de nombres de REDUNAM, una breve explicación de lo que es NICunam y su importancia en la administración de cada uno de los cuatro servidores de nombres, así como también las políticas que se tienen en la asignación de direcciones IP, dominios y DNS.

CAPITULO 1 "CONCEPTOS GENERALES"

En el presente capítulo se dará una breve explicación de los temas y de los conceptos que ayudaran a entender mas claramente el tema principal de este trabajo de investigación.
Los temas a desarrollar son únicamente dos; el primero, que es Internet, abarcará su definición, su historia, así como el auge que tiene en nuestro país.
Por otro lado, en el desarrollo de este tema, se podrá ver la gran importancia que tiene el DNS (Sistema de Nombres de Dominio) en el funcionamiento de Internet, no solo en REDUNAM, sino en todo el mundo; puesto que por medio de él, se hace posible el mapeo entre las direcciones IP y los nombres de dominio.
El segundo tema tratado en el capítulo corresponde a TCP/IP, protocolo importante en el mundo de Internet, el cual ayudará a entender el proceso de la transmisión de los datos para que puedan llegar de un lugar a otro.

1.1 INTERNET

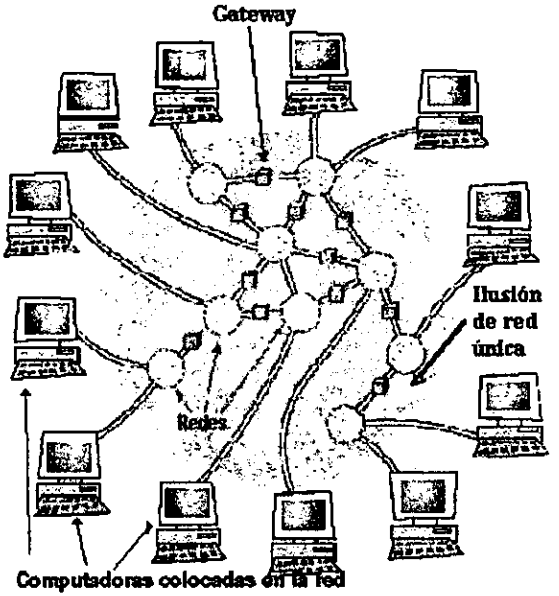
1.1.1 Introducción a Internet

Internet es un conjunto de redes locales conectadas entre sí a través de un ordenador especial por cada red, conocido como *gateway*[1]. Las interconexiones entre *gateways* se llevan a cabo a través de diversas vías de comunicación, entre las que se encuentran líneas telefónicas, fibras ópticas y enlaces por radio, que forman las vías principales.
También en ocasiones en esta gigantesca red los datos pueden transmitirse vía satélite, o a través de servicios como la telefonía celular.
En cierto modo, no hay mucha diferencia entre Internet y la red telefónica que todos conocemos, dado que sus fundamentos son parecidos. Como por ejemplo, basta identificar algunos servicios o sistemas a los que se pueda tener acceso a través de algún tipo de conexión, como un ordenador personal, una base de datos en una universidad, un servicio de pago, un fax o un número de teléfono, pueden ser, y que de hecho todo esto forma parte de Internet.
Internet es la Red de Redes, lo que quiere decir que diferentes redes operadas por una multitud de organizaciones están conectadas entre sí para formar Internet, lo que les permite comunicarse, intercambiar recursos, y compartir datos con otros usuarios alrededor del mundo.
Desde el punto de vista de un usuario, Internet representa una gigantesca red de información, en la que se puede encontrar una gran variedad de temas, además de una gran colección de programas, imágenes, sonidos y elementos multimedia que pueden obtenerse a través de herramientas adecuadas.
Lo interesante es que cada vez más de estos servicios están disponibles a través de Internet: fax, teléfono, radio, televisión, imágenes de satélites o cámaras de tráfico son algunos ejemplos.

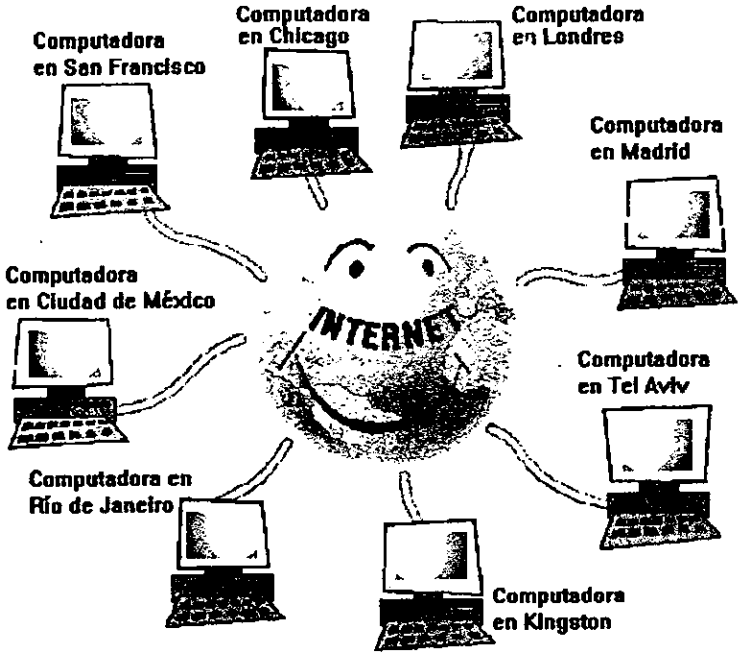
---

[1] Gateway, en redes, es un conexión compartida entre una red de área local (LAN) y un sistema más grande, tal como una maxicomputadora o una red de conmutación de paquetes.

Actualmente Internet está formada por millones de computadoras y aproximadamente 117 millones[2] de usuarios en todo el mundo conectados a ella de todas partes del mundo a través de todo tipo de computadoras y medios de conexión utilizando un mismo lenguaje, el protocolo TCP/IP.
En cuanto a organización, Internet no tiene en realidad una cabeza central, ni un único organismo que la regule o al que pedirle cuentas si funciona mal. Existen redes privadas que son totalmente propietarias, administradas y mantenidas por las propias empresas, aunque muchas veces, los medios de transmisión son provistos por otros organismos o instituciones. También están las redes públicas, que son usadas, mantenidas y tarificadas por *carriers*, quienes ofertan sus servicios de red al público en general.
Como Internet está formada por muchas redes independientes, que hablan el mismo lenguaje, ni siquiera están claros sus límites.
La mayor ventaja de Internet es que es una herramienta que provee el acceso a una amplia cantidad de información en línea y a bajo costo a lo largo y ancho del mundo.
En las siguientes gráficas, se puede apreciar a grandes rasgos, la idea que los usuarios tienen de la estructura de Internet.



[2] Existen a la fecha (diciembre de 1998) 117 millones de usuarios de Internet en todo el mundo de los cuales 84 millones utilizan el servicio WWW(World Wide Web), cifra que va aumentando cada día. La taza anual de crecimiento de usuarios es del 65%.
Http://www.khainata.com/extrainternet/int.html



1.1.2 Historia de Internet

Internet surgió de la necesidad que el gobierno de los Estados Unidos tenía por resolver un problema de estrategia militar durante el periodo de la Guerra Fría.
RAN Corporation, una de las empresas encargadas de la estrategia militar estadounidense propuso una solución: crear una red de comunicaciones que no dependiera de un organismo central, que estuviera integrada por nodos[3] o puntos de enlace de igual rango y con la misma capacidad de originar, transmitir y recibir mensajes, de modo que si alguno de estos nodos recibiera un ataque o dejara de funcionar, el resto de la red pudiera seguir en operación. Los mensajes que fueran enviados a través de esta red se dividirían en paquetes y cada uno de ellos tendría su propia dirección: se originarían en algún nodo en particular, saltarían de lado a lado hasta llegar a otro nodo específico, de manera individual. La ruta que siguieran los paquetes realmente no importaba; lo importante era que

[3] Un nodo es cualquier dispositivo conectado a la red

llegaran. Si una ruta hubiera sido destruida, el paquete encontraría otro camino para llegar a su destino.

La planeación de este tipo de redes se expuso durante un simposio en 1967 realizado en Inglaterra sobre Principios Operativos y fue apoyada por la ACM (*Asociation of Computer Machinery*).

En 1969 ARPA (*Advanced Research Projects Agency*), una agencia del Pentágono que surgió a partir del lanzamiento del satélite *Sputnik*, decidió realizar un proyecto mayor sobre una nueva tecnología en redes en los Estados Unidos. El proyecto fue desarrollado por RAND, MIT (*Massachussets Institute of Technology*) y UCLA (*University of California Los Angeles*). El primer nodo fue instalado en UCLA. Para diciembre de ese año ya existían cuatro nodos de ARPANET desde donde se podían transmitir datos y programar computadoras de otros nodos. En 1971 había quince nodos y para 1972, treinta y siete.

Poco a poco comenzó a expandirse el uso de ARPANET; no solamente se dedicaba a trabajos de cómputo a larga distancia, sino que se extendió a la comunicación de proyectos y trabajos entre investigadores y al uso personalizado del correo electrónico.

En 1973 tuvo lugar la primera conferencia internacional de ARPANET, en la que se dio una demostración con 40 máquinas conectadas entre sí alrededor del mundo; no hubo ninguna pérdida de información y en general la demostración tuvo un éxito impresionante.

Otra ventaja de ARPANET era que no importaba el tipo o tamaño de las máquinas en las que se estuviera trabajando, mientras cumplieran con los protocolos establecidos, funcionarían dentro de la red.

El protocolo original se conocía como NCP (*Network Control Protocol*); se cambió después por un nuevo estándar más sofisticado llamado TCP/IP y que en 1974 fue publicado por Vint Cerf y Bob Kahn.

Hacia el año de 1977 comenzó a extenderse el uso de TCP/IP en otras redes para vincularse a ARPANET y esta red comenzó a volverse pequeña en comparación con la gran cantidad de máquinas que empezaron a conectarse.

A fines de los años 70 y en los años 80 personas de diferentes grupos sociales, tuvieron acceso a computadoras de gran capacidad y era fácil conectarse a la creciente red de redes.

Como el software de TCP/IP era de dominio público y por su misma naturaleza, descentralizante y hasta anárquico, comenzó el auge de la conexión a Internet. Fue en esta época cuando surgió USENET, el boletín electrónico más grande del mundo, éste utilizaba el sistema operativo UNIX, que, al paso de los años, se ha convertido en el sistema operativo estándar de todas las computadoras de mediano y gran tamaño conectadas a Internet.

El departamento de Defensa de los Estados Unidos declaró como estándar al conjunto TCP/IP y separó de ARPANET la parte militar. Se dio entonces el auge de las estaciones de trabajo de escritorio, con sistema operativo *Berkeley* UNIX, que incluía software de red TCP/IP.

En 1984 la NFS (*National Sciencie Fundation*), a través de su oficina de Cómputo Científico Avanzado, estableció un nuevo avance técnico al integrar 5 supercomputadoras de enlace más rápido, lo que impulsó el desarrollo de Internet y permitió una mayor cantidad de conexiones, principalmente de universidades, con finalidades académicas y de investigación.

En este punto se inició la organización de los dominios (o direcciones de Internet para las diferentes redes conectadas), de los cuales ya se hablará más adelante.

Empezaron a surgir problemas en la red, como el caso del virus de Internet que aprovechaba un error en el código de los programas de correo electrónico y afectó a 6,000 de las 60,000 computadoras conectadas a Internet. Por este motivo, DARPA creó CERT (*Computer Emergency Response Team*), que generaba recomendaciones y alertas en caso de problemas dentro de la red.
En 1989 México ingresó a Internet a través de NSFNET y contaba además con la red BITNET, que permitía a usuarios del ITESM (Instituto Tecnológico de Estudios Superiores de Monterrey) y la UNAM (Universidad Nacional Autónoma de México) tener acceso a los recursos existentes en Estados Unidos y el resto del mundo.
Por iniciativa de los usuarios, surgieron las primeras organizaciones dedicadas a la protección de los derechos de las personas conectada a Internet. Este es el caso de EFF (*Electronic Frontier Foundation*) y de la primera organización que comercializa el acceso a Internet vía modem: *The World*.
También se implementaron herramientas que catalogan y facilitan el acceso a Internet: Archie, para la búsqueda de archivos accesibles mediante FTP (*File Transfer Protocol*) y Hytelnet, un catálogo de recursos y bibliotecas en línea.

1.1.3 Internet en México

La historia de Internet en México empieza en el año de 1989 con la conexión del Instituto Tecnológico y de Estudios Superiores de Monterrey, en el Campus Monterrey, ITESM hacia la Universidad de Texas en San Antonio (UTSA), específicamente a la escuela de medicina, por medio de una línea privada analógica.
Sin embargo, entes de que el ITESM se conectara a Internet, casi a final de los años 80, recibía el tráfico de BITNET por la misma línea privada. El ITESM era participante de BITNET desde 1986.
Pero la UNAM no podía quedarse atrás en el desarrollo de las comunicaciones por lo que en 1987 la Universidad Nacional Autónoma de México se conecta a BITNET.
La máquina que recibía la conexión de DECNET era una Microvax-II con la dirección 131.178.1.1. Esta máquina tenía un software que recibía el tráfico de TCP/IP encapsulado en DECNET, lo sacaba y permitía tener acceso a Internet.
Esta máquina fue también el primer Name Server o Servidor de Nombres para el dominio .mx.
El nodo de conexión a Internet de la UNAM, se localizaba en el Instituto de Astronomía en la Ciudad de México. Esto mediante una conexión vía satélite de 56 Kbps, con el Centro Nacional de Investigación Atmosférica (NCAR) de Boulder, Colorado, en los Estados Unidos de Norteamérica. Por lo tanto, se trataba de una línea digital.
Después de esto, lo que proseguía era una interconexión entre la UNAM y el ITESM (Campus Monterrey), pero lo que funcionó en ese momento fue un enlace BITNET entre ellos.
El ITESM, en su Campus Estado de México, se conectaba a través del Centro de Investigación Atmosferica (NCAR) a Internet. Como la UNAM, obtiene una conexión satelital de 56 Kbps, es decir, enlace digital. La función de este enlace es dar servicio a los demás ITESM, distribuidos a través de todo el país.

El ITESM, Campus Monterrey, promovió y logró que la Universidad de la Américas (UDLAP) en Cholula, Puebla y el Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO) en Guadalajara, Jalisco, se enlazaran a INTERNET a través del mismo ITESM.
Aunque sus enlaces eran de baja velocidad, 9600 bps, fue suficiente, en ese momento, para proveer de correo electrónico, transferencia de archivos y acceso remoto.
Debido al crecimiento registrado en Internet, la *National Science Fundation*, en los Estados Unidos, requería de una respaldada red de telecomunicaciones para todos aquellos países que se integraban a Internet, por lo tanto, se tomaron algunas decisiones en México, como la de formalizar el uso de IGRP entre los ruteadores y revisar detalladamente la asignación de ASN[4] (*Authonomous Systems/Sistema Autónomo*).

Formación de MEXNET

En este entonces existía un organismo llamado RED-MEX, formado principalmente por la academia, y es donde se discuten las políticas, estatutos y procedimientos que habrían de regir y dirigir el camino de la organización de la red de comunicación de datos de México. Esta debería ser una Asociación Civil.
Es así (después de muchos problemas para reunir a los representantes legales de cada institución) como surge MEXNET.
El 20 de enero de 1992 en la Universidad de Guadalajara, se reúnen los representantes de el ITESM, Universidad de Guadalajara, Universidad de las Américas, ITESO, Colegio de Postgraduados, LANIA, CIQA, Universidad de Guanajuato, Universidad Veracruzana, Instituto de Ecologia, Universidad Iberoamericana, IT de Mexicali; todos con un motivo en común, el cual era el de crear a la Asociación Civil.
Años mas tarde, BAJAred se empieza a formar con las siguientes instituciones educativas, todas ellas de Baja California:
Centro de Enseñanza Técnica y Superior - CETYS.
Centro de Investigación Científica y Educación Superior de Ensenada - CICESE.
Universidad Autónoma de Baja California - UABC.
Colegio de la Frontera Norte - COLEF.
Instituto Tecnológico de Mexicali - ITM
Es en 1993 cuando la UAM se establece como el primer NAP, al intercambiar tráfico entre dos diferentes redes.
Para finales de 1993 existían una serie de redes ya establecidas en el país, algunas de ellas:

MEXnet
RedUNAM
Red ITESM
RUTyC, que desaparecería como tal ese mismo año
BAJAnet
Red Total CONACYT
SIRACyT, un esfuerzo por agrupar las anteriores

[4] Conjunto de redes y ruteadores que cambian información de ruteo mediante el uso de un protocolo de ruteo.

Fue hasta 1994, con la formación de la Red Tecnológica Nacional (RTN), integrada por MEXnet y CONACyT que el enlace creció a 2Mbps (E1). Y es en este año que Internet se abre a nivel comercial en nuestro país con PIXELnet, ya que hasta entonces, solamente instituciones educativas y de investigación lograron realizar su enlace a Internet.
Durante 1994 y 1995, se consolidaron redes como RTN creando un *Backbone*[5] nacional y agrupando a un gran numero de instituciones educativas y comerciales en toda la República, desde Baja California hasta Quintana Roo. Se mantuvieron esfuerzos de RedUNAM y surgieron los ISP's (Proveedores de Acceso a Internet) comerciales con más fuerza, los cuales no sólo brindaban conexión a Internet sino servicios de valor agregado, tales como acceso a Bases de Datos públicas y privadas.
En Diciembre de 1995 se hace el anuncio oficial del Centro de Información de Redes de México (NIC-México) el cual se encarga de la coordinación y administración de los recursos de Internet asignados a México, tales como la administración y delegación de los nombres de dominio ubicados bajo .mx.
Nace la Sociedad Internet, Capítulo México, una asociación internacional no gubernamental no lucrativa para la coordinación global y cooperación en Internet. Se crea el *Computer Emergency Response Team* de México
A finales del 96 la apertura en materia de empresas de telecomunicaciones y concesiones de telefonía de larga distancia provocó un auge momentáneo en las conexiones a Internet, por lo que empresas como AVANTEL y Alestra-AT&T competían con TELMEX.
En 1997 existían más de 150 Proveedores de Acceso a Internet que brindaban sus servicios en el territorio mexicano y que se encontraban ubicados en los principales centros urbanos como: Cd. de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Mérida, Nuevo Laredo, Saltillo, Oaxaca, por mencionar sólo algunos.

1.1.4 NIC-México

El Network Information Center/ Centro de Información de la Red - México, (NIC-México) es la organización encargada de la administración del nombre de dominio nacional, el código de dos letras asignado a cada país según el ISO 3166.
Entre sus funciones están el proveer los servicios de registro y asignación de recursos de Internet para México, tales como nombres de dominio bajo el nTLD (national Top Level Domain) o direcciones IP, así como el mantenimiento de las bases de datos respectivas a cada recurso.
Este nace el 1ro. de Febrero de 1989, cuando el ITESM, Campus Monterrey realiza su conexión directa al Internet. En esos momentos se conecta la máquina a Internet bajo el dominio .mx: dns.mty.itesm.mx con la dirección 131.178.1.1.

[5] En comunicaciones, parte de la red que maneja el grueso del tráfico. La columna vertebral [backbone] puede conectar diferentes edificios (o ubicaciones) y otras redes más pequeñas que se pueden incluir en ella.

Esta máquina, una Microvax-II, digital, fue el primer servidor de nombres para el dominio .mx. Lo fue hasta el 6 de Septiembre de 1993 (fecha del 50 aniversario del sistema ITESM), la sustituyó una Sun SPARC Classic con 48 MB en RAM y 400 MB en disco.
En ese entonces no se requirió de una administración dedicada, ya que no existían muchos nombres de dominio ya que para 1992 había sólo 45 dominios bajo .mx, de los cuales 40 eran académicos y 5 eran comerciales.
Incluso este nTLD fue plano hasta octubre de 1993, cuando en una reunión de los principales actores de las redes en México, la SyRACyT se acordó crear los subdominios com.mx, gob.mx, y es en esa misma junta (en la Universidad de Monterrey) donde se decide NO crear el subdominio edu.mx. A principios de 1995 eran poco más de 100 nombres de dominio ubicados bajo .mx.
Después del éxito del WWW, se registró un incremento considerable en el número de dominios registrados mensualmente, lo que requirió una administración dedicada, así como la puesta en marcha de algunos servicios, tales como: registro en línea de nombres de dominio, solicitud de IP, registro de ISP en el país; todo ello a través páginas de WEB.
En octubre de 1995, se hace oficial la designación del ITESM, Campus Monterrey como NIC para México, lo que hace oficial el trabajo que se había venido desarrollando desde 1989.
En diciembre de 1995 se hace el anuncio oficial del NIC-México, para entonces se contaba con servicios de listas de correo y FTP anónimo. A finales de este año había ya 326 nombres de dominios bajo .mx.
Durante 1996 se adquiere un nuevo equipo, una SUN SPARC 20, 256 MB RAM y se empiezan a desarrollar servicios de registro automatizados y eficientes. A finales de este año ya se había aumentado a 2838 nombres de dominios bajo .mx.
El crecimiento acelerado en el número de dominios hizo necesario un mantenimiento de Bases de Datos actualizadas y en línea para la operación diaria de Internet en México, por lo que NIC-México evoluciona y en enero de 1997 empieza a funcionar la Base de Datos WHOIs para el dominio .mx. Durante este año se fijan cuotas de cobro por registro y mantenimiento de los dominios. El total de dominios registrados hasta 1997 era de 7251.
Debido a ese crecimiento, la UNAM decide hacer la petición ante NIC-México para poder tener un servidor de nombres secundario para el dominio .mx. Se estudia su situación, y al comprobar que cumplía con los requisitos, que se muestran a continuación, el 17 de junio de 1998 se le concede el derecho para que ns.unam.mx funja como servidor de nombres secundario.

Requisitos para un servidor secundario de .mx

- Usar BIND e su versión estable más actualizada.
- Sistema dedicad solo a proveer servicios de DNS, esto con el fin de asegurar que su eficiencia no se vea disminuida porque otros servicios están consumiendo los recursos del sistema.
- Deben estar en el servidor solo las cuentas de quienes lo administran; para reducir al máximo la posibilidad de accesos indeseables a la información y el DNS.
- En el servidor se debe instalar un sistema de monitoreo del DNS en la red, de tal forma que se puedan conocer la cantidad de peticiones que atiende por minuto y la ocupación de los enlaces.

- Por razones de seguridad y eficiencia se deben limitar las transferencias de aquellos servidores a los que el NIC-México explícitamente les haya autorizado hacerlo, impidiéndoselo a cualquier otra máquina.
- El servidor debe estar físicamente ubicado en un lugar con acceso restringido.
- Debe contar con fuentes de energía redundantes que le permitan mantener una operación constante.
- Los cortes de energía deben ser reportados con al menos 24 horas de anticipación, en caso de que esto no sea posible, o que el evento haya sido imprevisto, se debe avisar telefónicamente a la administración del NIC-México.
- Los administradores del servidor y la red que le da servicio deben mantenerse actualizados acerca de las posibles amenazas de seguridad que se puedan presentar como también deben estar prontos a la implementación de soluciones para prevenirlas y combatirlas.

Actualmente hay cuatro servidores oficiales para .mx y subdominios:

① ns.nic.mx
② mex1-m-213.uninet.net.mx
③ dns1.avantel.net.mx
④ ns.unam.mx ← NICunam

Los dos últimos no se encuentran administrados directamente por NIC-México.

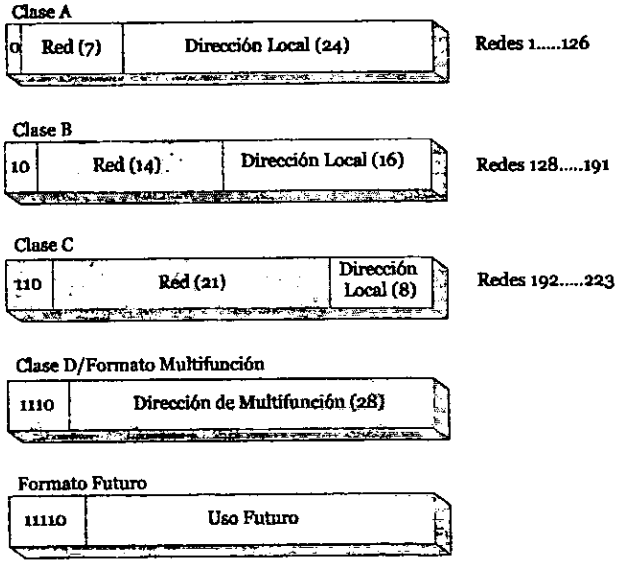
1.1.5 Nombres y Direcciones

Para navegar por Internet, lo primero que se debe saber es: ¿Qué es una dirección?, ya que para tener acceso a los servicios dentro de la red, siempre habrá que especificar al menos una.
En Internet, la palabra dirección se refiere siempre a una dirección electrónica, no a una dirección postal.
Todas la máquinas conectadas a Internet, tienen una dirección numérica única e irrepetible, llamada dirección IP y sirve para poder comunicar a una máquina con otras. La dirección no se asigna arbitrariamente, se debe hacer una petición al *Network Information Center* (NIC), el cual es el organismo responsable de la administración de las direcciones de toda la red y utilizar las que ya se hayan asignado.
Las direcciones se componen de cuatro octetos (grupos de números) separados por puntos. Por ejemplo, la dirección 132.248.204.5 corresponde al servidor ars.nic.unam.mx de la Dirección General de Servicios de Cómputo Académico (DGSCA).
La dirección de Internet (*IP address*) se utiliza para identificar tanto a una computadora en concreto como a la red a la que pertenece, de manera que sea posible distinguir a las computadoras que se encuentran conectadas a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de diversos tamaños, se establecieron tres diferentes clases de direcciones, las cuales se representan mediante tres rangos de valores:

- Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red,

quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de computadoras en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de clase A. Lo normal para las grandes organizaciones es que utilicen una o varias redes de clase B.

- Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64,516 computadoras en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que le número de computadoras que se necesita conectar fuese mayor, sería posible obtener mas de una dirección de clase B, evitando de esta forma el uso de una clase A.
- Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primero bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadoras en cada red. Estas direcciones permiten un menor número de host que las anteriores, aunque son las mas numerosas pudiendo existir un gran número de redes de este tipo (más de dos millones).



Formatos de Direcciones IP

En la gráfica anterior, en el número de redes, se puede notar que ciertos número no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clase D y E, que aun no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no puede usarse normalmente por tener otros propósitos específicos.

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de *host* para máquinas que aún no conocen su número de *host* dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el *broadcast* es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de *broadcast* es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del *broadcast* se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al *host*. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El *broadcast* es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible. En ARPAnet y en las líneas punto a punto no es posible enviar *broadcast*, pero sí que es posible hacerlo en las redes *Ethernet*, donde se supone que todos los ordenadores prestarán atención a este tipo de mensajes.

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (subredes). Como por ejemplo, podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de 2 bytes. En este caso, sería posible utilizar el tercer byte para indicar en que red *Ethernet* se encuentra un *host* en concreto. Esta división no tendría ningún significado para cualquier otro ordenador que esté conectado a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho más cómodo el acceso que si se tratara de varias direcciones de clase C independientes.

Una dirección para un servidor Internet, puede representarse tanto con una serie de números como con un nombre en forma textual. Los números y los nombres indican la misma dirección. Las computadoras usan el número para rutear los datos en Internet pero las direcciones numéricas son difíciles de recordar para el hombre, así que se inventó una forma para que en lugar de referirnos a las máquinas por medio de números lo hagamos a través de nombres. Por ejemplo, para la máquina, que anteriormente se había mencionado, su equivalente es: 132.248.204.5 ars.nic.unam.mx

en donde
ars es el nombre del servidor
nic es el grupo de máquinas que forman un dominio
unam dominio que hace referencia a la Universidad Nacional Autónoma de México (UNAM)
mx dominio que hace referencia a México

1.1.6 Dominios en Internet

En las secciones anteriores, ya se mencionó mucho la palabra dominio, concepto que se debe tener perfectamente claro, para poder entender el desarrollo de este trabajo.
El concepto de dominio, no es mas que un alias (o seudónimo) de una dirección IP.
Como nuevamente lo expresa el ejemplo que se ha venido utilizando,

132.248.204.5 ars.nic.unam.mx

el dominio ars.nic.unam.mx es el alias de la dirección IP 132.248.204.5.
Hay que tener especial cuidado con la distinción entre mayúsculas y minúsculas, dado que se consideran letras distintas y, por lo tanto, direcciones distintas, así como con la presencia de espacios en blanco dentro de la dirección. Las distintas partes que forman el dominio reciben el nombre de subdominios. El subdominio de más alto nivel del nombre de una máquina es la serie de letras que se encuentran al extremo derecho del dominio, y se le conoce como dominio raiz, dominio de primer nivel o top level-domains (TLD).
El dominio raíz indica el tipo de organización o país a la que dicha dirección pertenece. Con este dominio, el usuario puede intuir a que tipo de organización o país pertenece la máquina a la que se está conectando.
Existen dos tipo de dominios de primer nivel, los dominios de organizaciones y los dominios geográficos.
☛Dominios geográficos, Cada país se representa por dos caracteres de acuerdo con el código internacional de los países, según los estándares de la ISO (*International Standart Office*). De tal manera que si vemos una dirección como esta:

usuario@deimos.unam.mx

sabríamos que este usuario se encuentra en México.
La siguiente es una tabla de algunos dominios geográficos:

mx	México	**jp**	Japón
ca	Canadá	**au**	Australia
ch	Suiza	**de**	Alemania
dk	Dinamarca	**es**	España
fr	Francia	**tr**	Turquía
il	Israel	**pl**	Polonia
uk	Reino Unido	**us**	Estado Unidos

☛Dominios de Organizaciones, existen además otras divisiones para los dominios de más alto nivel que fueron las primeras divisiones que hubo en Estados Unidos para diferenciar el tipo de organización que se conectaba a la red. Estos dominios son los siguientes:

com	Organización Comercial
edu	Instituciones Educativas
gov	Instituciones gubernamentales
int	Instituciones Internacionales
mil	Instituciones Militares
net	Instituciones que regulan y dan servicio a la red
org	Organizaciones no lucrativas

Todas las redes que se conectan a Internet lo hacen de manera voluntaria, por esto nadie controla Internet. Todo lo que se publica en Internet es de dominio público, pero existe una entidad alojada en el estado de Washington, E.U., a la que se le ha encomendado controlar la creación de puntos de entrada a Internet, esta institución se llama InterNIC, cuya función es catalogar y entregar licencias a toda persona o institución que desea participar en Internet.

1.2 TCP/IP

Protocolo es un lenguaje común estandarizado que hablan dos máquinas para entenderse entre ellas. El uso del protocolo TCP/IP[6] en todas las computadoras de Internet permite que cualquiera de ellas pueda comunicarse con otra.

1.2.1 Definición de TCP/IP

Se puede ver a Internet como una malla muy compleja, compuesta por miles de redes en todo el mundo unidas entre sí por conexiones de distintos tipos (líneas telefónicas, red digital integrada, enlace vía satélite, fibra óptica, cable coaxial, etc.) que utilizan un lenguaje común denominado TCP/IP, que ofrece una serie de servicios.
Para realizar la interconexión entre las redes se necesita un ruteador, que se encarga de controlar los datos que hay en las distintas redes.
La función que realiza el ruteador es la de recibir paquetes de información y enviarlos hacia el destino indicado. Dentro del paquete debe haber información de la dirección destino a la que hay que mandar dicho paquete y la dirección origen para que la máquina destino sepa quien le ha enviado el paquete.
La arquitectura TCP/IP proporciona, de una forma sencilla y fiable, la capacidad de que cualquier equipo conectado, a cualquier red, pueda conectarse con otro equipo conectado.
Los equipos pueden estar en cualquier parte del mundo, y pueden ser desde grandes estaciones multiusuario (UNIX, VMS, MV, etc.) hasta una computadora personal (PC, MAC, SILICON, etc.). TCP/IP puede correr sobre una red Ethernet, Token Ring, etc.
El cimiento de Internet es el protocolo TCP/IP, un protocolo de transmisión que asigna a cada máquina que se conecta un número específico, llamado dirección IP.
El protocolo TCP/IP sirve para establecer una comunicación entre dos puntos remotos mediante el envío de información en paquetes. Al transmitir un mensaje o una página con imágenes, por ejemplo, el bloque completo de datos se divide en pequeños bloques que viajan de un punto a otro de la red, entre dos números IP determinados, siguiendo cualquiera de las posibles rutas. La información viaja por muchos ruteadores intermedios a modo de repetidores hasta alcanzar su destino, lugar en el que todos los paquetes se reúnen, reordenan y convierten en la información original. Millones de comunicaciones se establecen entre puntos distintos cada día, pasando por cientos de ruteadores intermedios.
La gran ventaja de TCP/IP es que es inteligente. Como cada intercambio de datos está marcado con direcciones IP determinadas, las comunicaciones no tienen por qué cruzarse. Y si los paquetes no encuentran una ruta directa, los equipos intermedios prueban vías alternas. Se realizan comprobaciones en cada bloque para que la información llegue intacta, y en caso de que se pierda alguno de los paquetes, el protocolo lo solicita de nuevo hasta que se obtiene la información completa.

---

[6] TCP/IP: Transmission Control Protocol/ Internet Protocol (Protocolo de Control de Transmisiones/ Protocolo Internet)

TCP/IP es la base de todas las máquinas y software sobre el que funciona Internet: los programas de correo electrónico (e-mail), transferencia de archivos (FTP) y transmisión de páginas con texto e imágenes (HTML).

1.2.2 Modelo OSI

El modelo OSI (*Open System Interconnect, Reference Model*) es un modelo de referencia que sirve para asegurar la comunicación entre redes. Este modelo fue creado por la ISO (Organización Internacional de Normalización), y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas. Esta clasificación permite que cada estándar se desarrolle con una finalidad determinada, lo cual simplifica el proceso de desarrollo e implantación. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores. Los siete niveles del modelo OSI son los siguientes:

Aplicación	El nivel de aplicación es el destino final de los datos donde se proporcionan los servicios al usuario.
Presentación	Se convierten e interpretan los datos que se utilizarán en el nivel de aplicación.
Sesión	Encargado de ciertos aspectos de la comunicación como el control de los tiempos.
Transporte	Transporta la información de una manera fiable para que llegue correctamente a su destino.
Red	Nivel encargado de encaminar los datos hacia su destino eligiendo la ruta más efectiva.
Enlace	Enlace de datos. Controla el flujo de los mismos, la sincronización y los errores que puedan producirse.
Físico	Se encarga de los aspectos físicos de la conexión, tales como el medio de transmisión o el hardware.

Tomando al modelo OSI como referencia podemos afirmar que para cada capa o nivel que él define existen uno o más protocolos interactuando. La comunicación es entre pares (peer-to-peer), es decir, un protocolo de un nivel dialoga con el protocolo del mismo nivel en la computadora remota.

1.2.3 Arquitectura del modelo TCP/IP

En la actualidad, las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo la implantación real de una arquitectura puede diferir de este modelo. Las arquitecturas basadas en TCP/IP proponen cuatro capas en las que su correspondencia con el modelo OSI es la siguiente: la capa de aplicación de TCP/IP corresponde a las capas de aplicación, presentación y sesión de OSI; la capa de transporte de TCP/IP corresponde a la capa de transporte de OSI; la capa de Internet de TCP/IP corresponde a la capa de red y también se entrelaza con la capa de enlace de OSI, por último, la capa de acceso a la red de TCP/IP corresponde a las capas de enlace y física de OSI.
Como se puede ver TCP/IP es un protocolo independiente del medio físico de comunicación, sin embargo existen estándares bien definidos a los nivel de enlace de datos y físico que proveen mecanismos de acceso a los diferentes medios y que en el modelo TCP/IP deben considerarse en la capa de acceso a la red; siendo los mas usuales el proyecto IEEE802, Ethernet, Token Ring.
Supóngase que un usuario desea visitar la página http:www.nic.unam.mx/formas.html y así se lo indica a Netscape (que corre en la capa de Aplicación). Netscape le pedirá a la capa de transporte que cree una conexión de punto a punto con el servidor de Web en la computadora www.nic.unam.mx, la que utilizará para solicitar y recibir la página formas.html. A su vez, la capa de transporte utilizará los servicios de la capa de Internet (que se encarga principalmente de enviar y recibir paquetes de información), A su vez, la capa de Internet utilizará los servicios de la capa de acceso a la red, que se encarga de enviar a través de la red local o un ruteador la información de una computadora a otra.
Cada capa tiene funciones bien específicas que permiten que el proceso completo se lleve a cabo. A continuación se describen brevemente cada una de ellas.

Capa de Acceso a la Red

La capa de acceso a la red está implantada en el manejador (device driver) del sistema operativo y en la tarjeta de interfaz que conecta a la computadora con la red. Esta capa tiene a su cargo los detalles de la comunicación en la capa física, así como garantizar la confiabilidad de ésta. La capa de Internet entrega a la capa de acceso a la red paquetes de información llamados datagramas. Cada datagrama contiene la dirección IP de su destinatario. Entre las funciones principales de la capa de acceso a la red se encuentran las siguientes:

- Convertir los datagramas en tramas (*frames*). Esto se debe a que las tarjetas de red deben enviar la información encapsulada en forma de tramas.
- Convertir la dirección IP del destinatario en su dirección física. Cuando una computadora desea enviar una trama de una computadora a otra es necesario que conozca la dirección física de la computadora destinatario (cada tarjeta de red tiene una dirección única, a la que se le llama dirección física); esto se debe a que a este nivel, las direcciones IP no son significativas.
- Enviar la información a la otra computadora
- Convertir las tramas recibidas en datagramas para entregarlas a la capa de acceso a la red en el lado receptor.

Capa de Internet

Esta capa es el corazón de Internet. Su función principal es la entrega de paquetes (datagramas) de una computadora fuente a otra destino. Implanta algoritmos para evitar congestionamientos y para interconexión de redes (gateways y ruteadores). Toda la información que se transmite a través de Internet son datagramas IP. Esta capa no es confiable, es decir, no se encarga de verificar que un datagrama haya sido recibido o volverlo a mandar en caso de existir algún error.
El protocolo central de esta capa es el IP, del cual se hablará mas adelante.

Capa de Transporte

La función principal de esta capa es permitir la comunicación directa del remitente a los destinatarios. En esta capa actúa principalmente el protocolo TCP del cual también se hablará en este capitulo más adelante.
TCP otorga a la capa de aplicación una comunicación libre de errores punto a punto (de fuente a destino). Además TCP define un nivel de direccionamiento llamado puerto, que permite distinguir entre diferentes conexiones que estén realizando simultáneamente. Cada puerto es identificado con un número de 16 bits. Su uso es claramente ejemplificado por el modelo cliente-servidor. Para que el cliente pueda conectarse con el servidor, es necesario que el primero sepa dónde encontrar al segundo; para resolver este problema, varios números de puerto son asignado por IANA (Internet Assigned Number Authority, Autoridad Asignadora de Números de Internet). Esta agencia reserva números a los servicios que pueden ofrecer un servidor. Por ejemplo, el número de puerto del servicio ftp es el 21, el de telnet es el 23, el de Web es el 80. En general, los números de puerto entre 1 y 255 los asigna la IANA. Un cliente de Web sabe que para conectarse con un servidor (también Web), debe establecer por omisión una conexión TCP al puerto 80 de la máquina en cuestión.

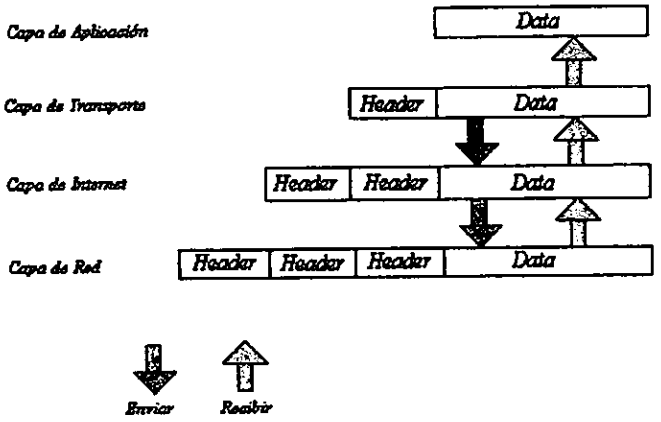
Capa de Aplicación

La capa de aplicación, como su nombre lo dice, es donde se encuentran las aplicaciones utilizadas por el usuario. Algunas aplicaciones son tan comunes que se decidió estandarizarlas, entre ellas se encuentran el acceso remoto (telnet, rlogin), la transferencia de archivos (ftp), el correo electrónico (SMTP), el Web (HTTP), etc..

1.2.4 Transmisión de paquetes

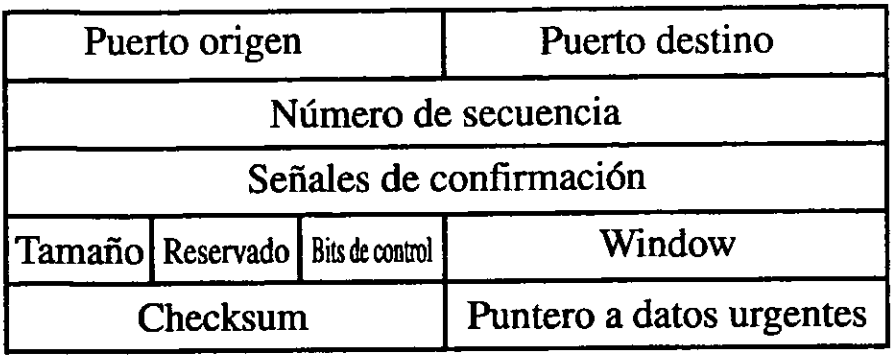
Así como en el modelo OSI, los datos son enviados a la red desde la capa mas alta hasta la mas baja del modelo y cuando se esta recibiendo la información, esta circula desde la capa mas baja hasta la mas alta. Cada capa en la pila, agrega información de control para asegurar que la información llegue correctamente.
A esta información de control se le llama header, ya que es colocada al inicio de los datos para ser transmitidos.

Cuando la información va atravesando cada capa, cada una de ellas, encierra la información obtenida de la capa anterior (tanto los datos originales como su cabecera o header) agregándole su propia cabecera, a este procedimiento se le llama encapsulamiento.
Cuando los datos son recibidos, sucede lo contrario, cada capa lee su cabecera correspondiente, antes de transmitir a la capa superior los datos, hasta llegar a la capa mas aita en la que ya son totalmente interpretados los datos.



1.2.5 Protocolo TCP (Transmission Control Protocol/Protocolo de Control de Transmisiones)

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño, en caso de ser necesario, y así poderse manejar más fácilmente. También se encargará de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.
La cabecera de un datagrama contiene al menos 160 bits que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea. Para llevar una organización de los datagramas, TCP los numera entes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar nuevamente el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.



Formato de la cabecera TCP

A continuación de la cabecera puede existir información opcional. En cualquier caso el tamaño de la cabecera debe ser múltiplo de 32 bits, por lo que se agregaría un campo de tamaño variable que contuviera ceros al final para conseguir que este objetivo se cumpla. El campo de tamaño contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa. Esto permite determinar el lugar donde comienzan los datos.

Dos campos incluidos en la cabecera y que son de especial importancia son los números de puerto origen y puerto destino. Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo ordenador puede estar utilizando varios servicios o transferencias simultáneamente, e incluso por medio de usuarios distintos.

El puerto de origen contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor debe tener asignado un número estándar para que pueda ser utilizado por el cliente.

Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas señales de confirmación una vez que se ha recibido y comprobado la información satisfactoriamente. Estas señales se incluyen en el campo apropiado de la cabecera del datagrama, que tiene un tamaño de 32 bits. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un periodo de tiempo razonable, el datagrama completo se volverá a enviar.

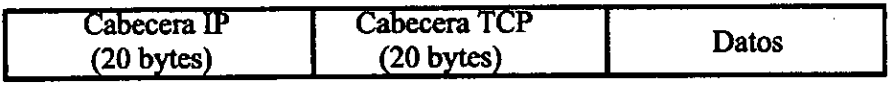
Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información llegue con errores a su destino. Para poder detectar cuando sucede esto se incluye en la cabecera un campo de 16 bits, en el cual al haber un error, se produce una alteración, a este campo se le conoce como checksum.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente. De esta manera el primero empezará por cero, el segundo contendrá un número que será igual al tamaño en bytes de la parte de datos del datagrama anterior, el tercero con la suma de los dos anteriores, y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.
Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada uno de los ordenadores puede procesar los datos que le son enviados. Si esto no se tuviera en cuenta, el ordenador de más potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla. Este inconveniente se soluciona mediante un campo de 16 bits (Window) en la cabecera TCP, en el cual se introduce un valor indicando la cantidad de información que el receptor está preparando para procesar. Si el valor llega a cero será necesario que el emisor se detenga. A medida que la información es procesada este valor aumenta indicando disponibilidad para continuar la recepción de datos.

1.2.6 Protocolo IP (Internet Protocol/Protocolo Internet)

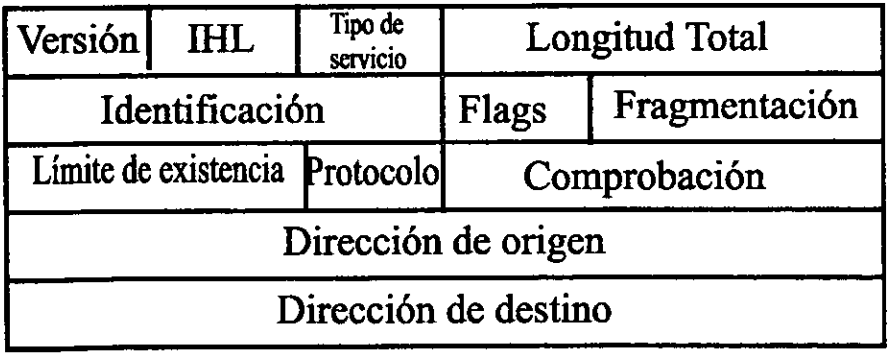
El IP es un protocolo que pertenece al nivel de red, por lo tanto, es utilizado por los protocolos del nivel de transporte como TCP para enrutar los datos hacia su destino. IP tiene únicamente la misión de enrutar el datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando. Suponiendo que el protocolo TCP ha sido el encargado de manejar el datagrama antes de pasarlo al IP, la estructura del mensaje una vez tratado quedaría así:



La cabecera IP tiene un tamaño de 160 bits y está formada por varios campos de distinto significado. Estos campos son:

- *Versión*: Número de versión del protocolo IP utilizado. La mayoría de los protocolos tienen este campo debido a que algunos nodos pueden no utilizar la última versión del protocolo disponible. La versión actual de IP es la 4. Tamaño 4 bits.
- *Longitud de la cabecera*: (Internet Header Length, IHL) Contiene cuatro bits con el valor de la longitud de la cabecera del datagrama. La longitud se mide en palabras de 32 bits. Tamaño 4 bits.
- *Tipo de servicio*: El tipo o calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. Tamaño 8 bits.
- *Longitud total*: Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bits, el tamaño máximo del datagrama no podrá superar los 64,516 bytes, aunque en la práctica este valor será mucho más pequeño. Tamaño 16 bits.

- *Identificación*: Valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño 16 bits.
- *Flags*: Indicadores utilizados en la fragmentación. Tamaño 3 bits.
- *Fragmentación*: Contiene un valor (offset) para poder ensamblar los datagramas que se hayan fragmentado. Está expresado en número de grupos de 8 bytes (64 bits), comenzando con el valor cero para el primer fragmento. Tamaño 16 bits.
- *Tiempo de vida*: Contiene un número que disminuye cada vez que el paquete pasa por un sistema. En esquemas reales, el TTL es una medida del número de saltos. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en una red correctamente diseñada, no debe descuidarse esta posibilidad. Tamaño 8 bits.
- *Protocolo*: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que puede ser tratado correctamente cuando llegue a su destino. Tamaño 8 bits.
- *Comprobación*: El campo de comprobación (checksum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia. Tamaño 16 bits.
- *Dirección de origen*: Contiene la dirección del host que envía el paquete. Tamaño 32 bits.
- *Dirección de destino*: Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño 32 bits.



CAPITULO 2 "SISTEMA DE NOMBRES DE DOMINIO (DNS)"

En este capítulo se explicará e ilustrará el mecanismo de trabajo del DNS. Se abordará en los conceptos o términos que se necesitan conocer antes de entrar a fondo en el funcionamiento del DNS en general, así como los pasos para la elaboración de los archivos necesarios para levantar un servidor de nombres.

2.1 HISTORIA DEL DNS

En los años 70, ARPANET fue una pequeña red con solo unos cuantos hosts. Un simple archivo, HOSTS.TXT, contenía toda la información que se necesitaba conocer sobre estos equipos; este archivo fue utilizado para mapear el nombre-dirección de cada host que estaba conectado a ARPANET.
Actualmente el archivo, utilizado sobre todo en equipos UNIX, que sirve de tabla de hosts es el /etc/hosts, que fue compilado del HOSTS.TXT.
El archivo lo mantuvo el SRI's Network Information Center y lo distribuía desde una simple máquina llamada SRI-NIC[7] .
Los administradores de ARPANET, típicamente notificaban al NIC de sus cambios por medio de correo electrónico, y periódicamente se conectaban a SRI-NIC para que por medio de ftp actualizaran su HOSTS.TXT.
Los cambios eran almacenados dentro de un nuevo HOSTS.TXT una o dos veces por semana. Así ARPANET creció, impresionantemente hasta que este esquema vino a ser incapaz de manejarse. El tamaño del HOSTS.TXT creció en proporción al aumento de hosts en ARPANET. Además, el tráfico generado por los procesos de actualización aumentaba considerablemente: cada nuevo host no significaba solo una línea en el HOSTS.TXT, sino que también era una actualización desde el SRI-NIC.
Cuando ARPANET adoptó el conjunto de protocolos de TCP/IP, la popularidad de la red creció. Para entonces, los problemas de los equipos con el HOSTS.TXT fueron:

- Carga de Tráfico

  El tránsito en la máquina SRI-NIC, en términos de tráfico y de carga en la red, llegó a ser incontrolable.

- Colisiones

  Dos hosts en el HOSTS.TXT no podían tener el mismo nombre. Sin embargo, aunque el NIC podía asignar direcciones, y de las cuales se garantizaba eran únicas, éste no tenía autoridad sobre los nombres de los hosts. Con esto no se pudo prevenir el tener conflictos con los nombres repetidos en la totalidad del esquema.

---

[7] SRI. Stanford Research Institute en Menlo PARK, California. SRI dirige investigaciones en diferentes áreas, incluyendo redes computacionales.

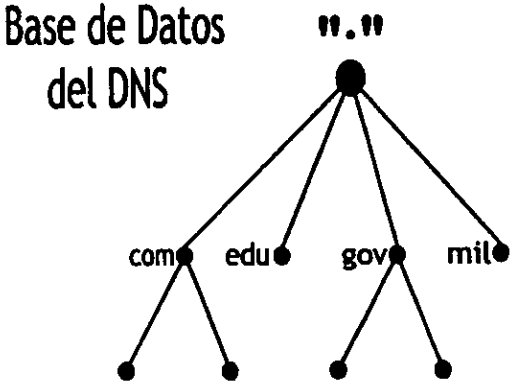
Alguien podía agregar un host con el mismo nombre al de un servidor de correo, por ejemplo, causando desorganización en el servicio de correo para muchos que se encontraran conectados a ARPANET.

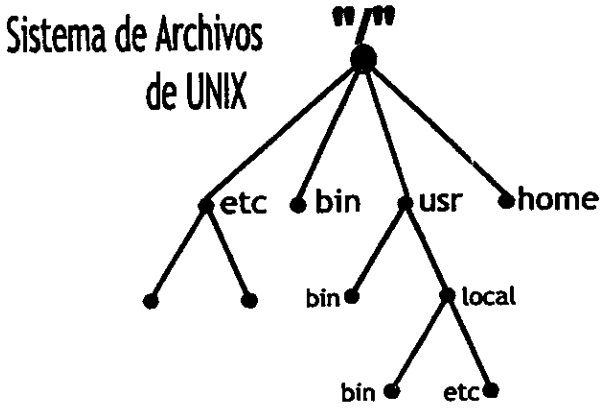
El principal problema fue que el mecanismo del HOSTS.TXT dejó de ser servicial, ya que irónicamente el éxito de ARPANET como experimento vino a ser el fracaso del HOSTS.TXT.
El gobierno de ARPANET, que se caracterizaba por estar orientado siempre a la investigación, y siendo los creadores del HOST.TXT, encontraron otra meta. Ésta consistía en tratar de crear un sistema que resolviera los problemas inherentes en el sistema de las tablas de host. El nuevo sistema tenía que permitir una administración local de los datos, pero al mismo tiempo permitir que dichos datos, siguieran disponibles para todos.
La descentralización de la administración podía eliminar un simple host y ayudar en el problema del tráfico.
Una administración local podía hacer que los medios para realizar el respaldo de los datos fueran mas fáciles.
Se podía usar un espacio de nombres jerárquicos de los host. Esto podía asegurar nombres únicos en los hosts.
Paul Mockapetris del USC's Information Sciences Institute, fue el responsable del diseño del nuevo sistema. En 1984, publicó el RFC 882 y el 883, en donde se describía el Sistema de Nombres de Dominio o DNS. Estos RFC's fueron reemplazados por el 1034 y 1035 respectivamente, que son las actuales especificaciones del sistema DNS.
Actualmente los RFC's se han aumentado al 1535, 1536 y 1537, en donde se describe el potencial del DNS en los problemas de seguridad, su implantación y administración.

2.2 Características del DNS y los Dominios

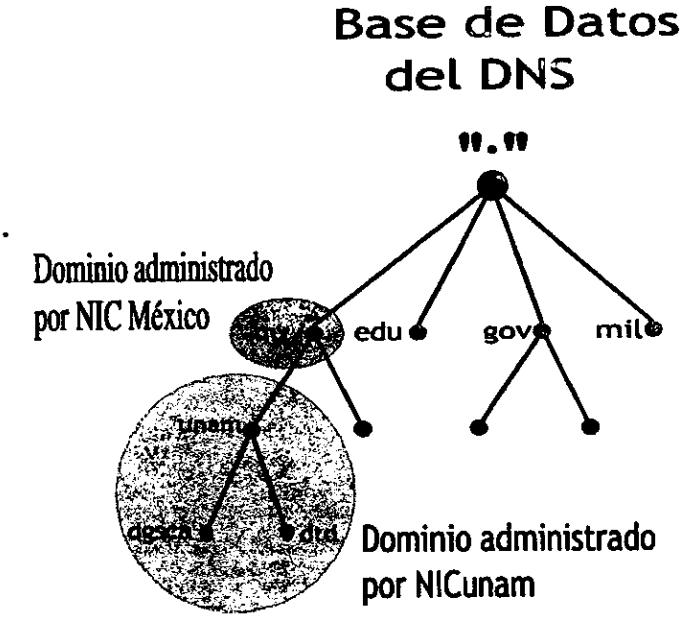
El Sistema de Nombres de Dominio es una base de datos distribuida. Esto permite un control local de los segmentos de toda la base de datos, sin embargo, los datos en cada segmento están disponibles a través de la red completa por medio del esquema cliente-servidor. Su protocolo le indica cómo convertir direcciones IP a nombres de dominio de las computadoras en la red y viceversa. El acceso a la base de datos del DNS se hace a través de las funciones "gethostbyname" y "gethostbyaddr", las cuales obtienen el nombre de la computadora o la dirección IP, respectivamente. Las computadoras que responden a dichas peticiones son llamadas servidores de nombres.
El servidor de nombres contiene información acerca de algunos segmentos de la base de datos y la hace disponible a los clientes llamados *resolvers*.
Los *resolvers* son rutinas que realizan las búsquedas enviándolas a través de la red al servidor de nombres.
Normalmente, toda computadora se comunica con uno o más servidores de nombres. Una de las características más sobresalientes del DNS es que no existe una computadora que contenga información sobre todos los nombres de las computadoras en Internet.

La estructura de la base de datos es dibujada como un árbol invertido, con la raíz en la cima. En UNIX, la raíz se representa por un slash (/). En el DNS, la raíz es representada por una etiqueta vacía (``) o simplemente con un (.).
Cada nodo en el árbol representa una partición de la base de datos completa, lo que sería un "directorio" en el sistema de archivos de UNIX, o un dominio en el Sistema de Nombres de Dominio. Cada dominio o directorio puede ser, a su vez, dividido en otras particiones llamadas subdominios en el DNS. Los subdominios son dibujados en el árbol como hijos de los nodos padre.
Cada dominio o nodo del árbol tiene una etiqueta. Esta etiqueta es con la que será identificado el dominio relativamente por los dominios padres. Esta etiqueta puede tener de hasta 63 caracteres de longitud. La secuencia de etiquetas de los nodos necesarios para ir desde un nodo hijo hasta el nodo raíz es conocido como el nombre de dominio de la computadora que corresponde a dicho nodo hijo. A cada sufijo de un nombre se le conoce también como un nombre de dominio. Por ejemplo, la computadora 132.248.204.5 tiene como nombre de dominio ars.nic.unam.mx y los nombres nic.unam.mx, unam.mx y mx son también nombres de dominio. Como se muestra en la siguiente figura.

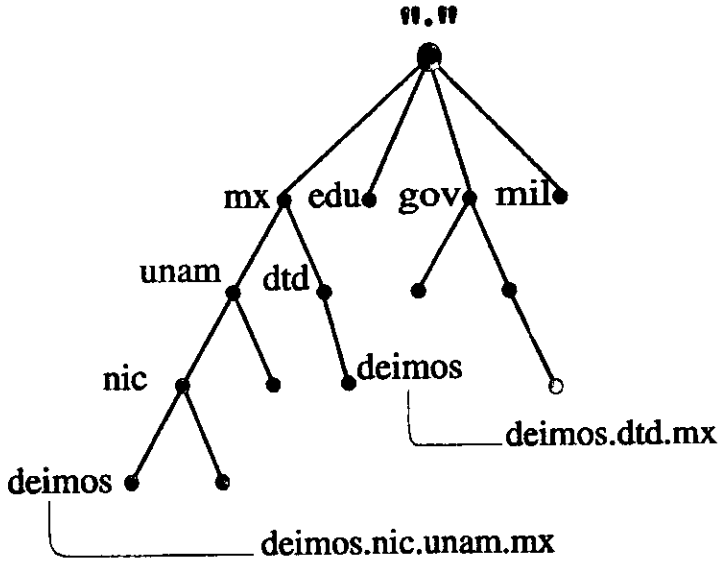




En el DNS cada dominio puede ser administrado por diferentes organizaciones. La administración de nombres de dominio en el primer nivel está a cargo de InterNIC. En el caso particular de México, cuatro de los dominios genéricos forman el segundo nivel del árbol como son com, gov, net y org. Por ejemplo, el Banco de México tiene el nombre de dominio banxico.org.mx; la empresa Internet de México, su nombre de dominio es internet.com.mx; el dominio edu no existe; pero existen algunas organizaciones que en lugar de registrarse con el NIC de México, decidieron hacerlo con el de EUA y, por lo tanto, tienen nombres de dominio como sar.net, bravo.net, etc. La administración del dominio mx está a cargo de NIC México: nic.mx. Cada organización puede dividir su dominio en subdominios y otorgar responsabilidades de estos subdominios a otras organizaciones. A este proceso se le conoce como "Delegación de Dominios".
Por ejemplo NIC México administra el dominio mx, pero delegó a la UNAM la administración del subdominio unam.mx, siendo específicamente su administrador NICunam
Esto se muestra en la siguiente figura.



Cada hots en la red tiene un nombre de dominio, el cual es un medio para tener la información sobre el host.
Esta información puede ser su dirección IP, información sobre ruteo, información de hardware, etc. Cada host puede tener uno o mas alias de nombres de dominio, que son simplemente apuntadores de un nombre de dominio a otro, ya sea el oficial o un nombre canónico.
Esta estructura se desarrolló para resolver el problema que el HOST.TXT tenía. Por ejemplo, creando nombres jerárquicos se elimina el peligro de las colisiones de los nombres.
Los dominios son dados únicamente por los nombres de dominio, así las organizaciones son libres de escoger el que deseen para sus dominios. Cualquier nombre que se escoja, éste no generará conflictos con otros nombres de dominio. Se pueden tener dos mismos nombres de dominio, por ejemplo deimos, pero cada uno tendrá diferentes dominios padre, que por consiguiente, hará que sean diferentes aunque tengan el mismo nombre.



Un dominio es simplemente un subárbol del espacio de dominios. Cualquier nombre de dominio en el árbol es considerado parte del dominio. Un dominio es un grupo de hosts. Los hosts son nombres de dominio que apuntan a información de hosts individuales.
Estos hosts están relacionados lógicamente, ya sea geográficamente u organizacionalmente, y no necesariamente por la red, dirección o tipo de hardware. Por ejemplo, podemos imaginar tener diez hosts; cada uno en diferente red, quizá en diferentes países, pero todos en el mismo dominio.
Los nombres de dominio en el interior del árbol pueden ser nombres de un host o pueden referirse a la estructura acerca de los dominios hijos, o subdominios. Interiormente, los nombres de dominio no están restringidos unos de otros. Ellos pueden representar a un dominio que les corresponda o a un host en particular en la red. Por ejemplo, hp.com es el nombre del dominio de Hewlett-Packard Company's y al mismo tiempo es el nombre del host que maneja el correo entre HP e Internet.

2.3 Servidores de Nombres

El programa que guarda la información acerca del espacio de dominios es llamado servidor de nombres. Generalmente un servidor de nombres, tiene la información completa sobre una parte del espacio de dominio, llamada zona.
Se dice que el servidor de nombres tiene autoridad sobre la zona. El servidor de nombres puede ser autoridad de múltiples zonas también.

Una zona es un subárbol del árbol del DNS que se administra por separado. Cada zona es dividida en subzonas. Por ejemplo, la UNAM dividió la administración de la red por departamentos (facultades, ENEP's, CCH's, etc). La organización responsable de cada zona está a cargo de proveer los Servidores de Nombres para dicha zona. Cada zona requiere de, por lo menos, dos servidores de nombres que respondan preguntas sobre la zona, uno de ellos debe estar localizado fuera de la red local, con lo que, aunque la red local no funcione, el DNS de la misma aún lo haga.
Cuando una computadora es agregada a una zona, el administrador se encarga de registrar su nombre y número IP notificando al Servidor de Nombres correspondiente.
Un ejemplo más claro es el del Departamento de Presupuesto de la UNAM; éste departamento tiene su administración local de su red, pero ellos tiene un servidor de nombres para su zona (solo para uso local), el cual resolverá para las máquinas de esa red, pero a su vez, también tienen configurados los cuatro servidores de nombres de NICunam, que en caso de que el servidor de nombres local falle, entrarán a substituirlo los otros, que se encuentran fuera de la red local.
Un servidor de nombres no necesita saber más que la información de zona de la que es responsable, y las direcciones de los servidores de las subzonas que define (en caso de que las haya) y las de los servidores de la zona padre de las que depende.

2.3.1 Tipos de servidores de nombres

Dentro de las especificaciones del DNS, se definen dos tipos de servidores de nombres, el primario y el secundario. El servidor de nombres primario es el que contiene los archivos de datos de los host que están corriendo en la zona para la cual el es autoridad. El servidor de nombres secundario obtiene los datos de su zona desde otros servidores de nombres, los cuales son autoridad para esa zona, o lo que es lo mismo, de los servidores primarios.
Cuando el servidor secundario se activa, éste contacta a otro servidor de nombres y si es necesario, obtiene los datos sobre la zona. A esto se le conoce como transferencia de zona.
El DNS se provee de estos dos tipos de servidores de nombres para hacer que la administración sea más fácil, puesto que al haber cambios, solo tiene que modificarse la base de datos del servidor primario, y los servidores secundarios se encargaran por ellos mismos de hacer la actualización.
Una vez que ya se hayan creado los datos para la zona y de haber inicializado el servidor de nombres primario, no es necesario que se copien los datos de un host a otro para crear un nuevo servidor de nombres para la zona. Simplemente hay que inicializar el servidor de nombres secundario y dejar que obtenga los datos del servidor de nombres primario.
Cuando los servidores ya se encuentren funcionando, el servidor secundario realizará consultas periódicamente al servidor primario para actualizar y guardar los datos de la zona.
Esto es muy importante, porque se puede tener mas de un servidor de nombres secundario en cualquier zona. Permitiendo que se tenga redundancia, distribución de la carga así como también tener la seguridad de que todos los hosts de la zona, tendrán un servidor de nombres siempre disponible.
Usando servidores de nombres secundarios, se puede tener una administración mas fácil de manejar.

Se había mencionado que un servidor puede ser autoridad en más de una zona. Similarmente, un servidor de nombres puede ser primario para una zona, y secundario para otra. Un servidor de nombres puede ser de los dos tipos, pero en diferentes zonas.
Puede haber varios servidores de nombres, pero dependiendo del orden en que se enlisten, va a ser el orden en que se haga la petición.

2.3.2 Archivos de datos

Los archivos de los servidores de nombres primarios cargarán los datos de la zona desde donde son llamados, ya sean los archivos de datos o los archivos de las zonas.
Los servidores secundarios están configurados para tener un respaldo de los datos de la zona, que transfieren desde los archivos de datos de los servidores de nombres primarios.
Si el servidor secundario se desconecta y luego se restablece su comunicación, éste leerá primero los archivos de respaldo, y verificará si se realizó alguna actualización.
Cuando se necesite llevar a cabo una transferencia de zona de los datos, y el servidor primario se encuentre deshabilitado, el secundario es el que proveerá los datos hasta que se restablezca el primario.
Los archivos de datos, contienen grabados los recursos que describen las zonas. Los recursos describen todos los hosts de la zona, e indican cuando se hizo una delegación de subdominios.

2.4 RESOLUCIÓN

Los servidores de nombres son expertos en recobrar los datos del espacio de dominios. Ellos tienen que serlo, puesto que de cierta manera son la inteligencia de los resolvers.
No solo tienen que brindar los datos de las zonas para las que son autoridad sino que también tienen que buscar en el espacio de dominios para los que no son autoridad. A este proceso se le llama *resolución de nombres* o simplemente *resolución*.
Debido a que la estructura del espacio de nombres es un árbol invertido, el servidor de nombres necesita solo un pedazo de información para encontrar el camino a cualquier punto del árbol; el nombre y la dirección de los *servidores de nombres de la raíz* o también conocidos como *root servers*.
Un servidor de nombres puede emitir una búsqueda a los servidores de nombres de la raíz para cualquier nombre de dominio y éstos servidores comenzarán con los servidores de nombres en este camino.

2.4.1 Servidores de nombres de la raíz (root servers).

Los servidores de nombres de la raíz conocen cuales son los servidores de nombres que son autoridad para los Top-level-domains.(en efecto, la mayoría de los servidores de nombres de la raíz, son autoridad para los top-levels). Al lanzar una búsqueda de cualquier nombre de dominio, los servidores de nombres de la raíz podrán proveer por lo menos la lista de los nombres y direcciones de

los servidores de nombres que son autoridad para el top-level domain del nombre de dominio en el que están.
Después, el servidor de nombres del Top-level, proveerá la lista de los servidores de nombres que son autoridad para el segundo nivel de dominios del nombre de dominio en el que están.
Cada servidor de nombres buscará y brindará la información de como conseguir la respuesta que busca, o bien darse la respuesta él mismo.
Se puede ver claramente que los servidores de nombres de la raíz son los más importantes en la resolución, por lo que el DNS provee un mecanismo para ayudar a disminuir la carga en los servidores de nombres de la raíz. Pero debido a la ausencia de información, la resolución no empieza en los servidores de nombres de la raiz. Esto ocasiona que en dichos servidores exista una operación crucial en el DNS. Si todos los servidores de nombres de la raíz en Internet fueran inalcanzables por un extenso periodo, toda la resolución en Internet sería un fracaso.
Para protegerse contra esto, Internet tiene 9 servidores de nombres de raíz, que están distribuidos en varias partes de Internet; entre los que se encuentran el localizado en España, en la NASA, en Europa y otro esta corriendo en un proveedor comercial de Internet, por ejemplo.
Uno de los temas que más preocupan en relación a estos servidores, es el tráfico tan alto que recibe cada uno de ellos por el gran número de consultas que se realizan. En un reportaje sobre un estudio realizado en 1992 por la U.S.C. se observó que los servidores de nombres de la raíz, recibían alrededor de 20,000 consultas en una hora, o lo que corresponde a seis consultas en un segundo aproximadamente.
En una mas reciente estadística realizada por InterNIC muestran que su servidor de nombres de raíz, ns.internic.net, recibía 255,600 consultas por hora o bien 71 consultas por segundo.
A pesar de la carga sobre los servidores de nombres de la raíz, la resolución en Internet es muy buena.
En la siguiente figura, se muestra el proceso de resolución para una dirección de un host y un dominio reales, en el que se incluye el proceso que corresponde al viaje de los dominios en el espacio de dominios.

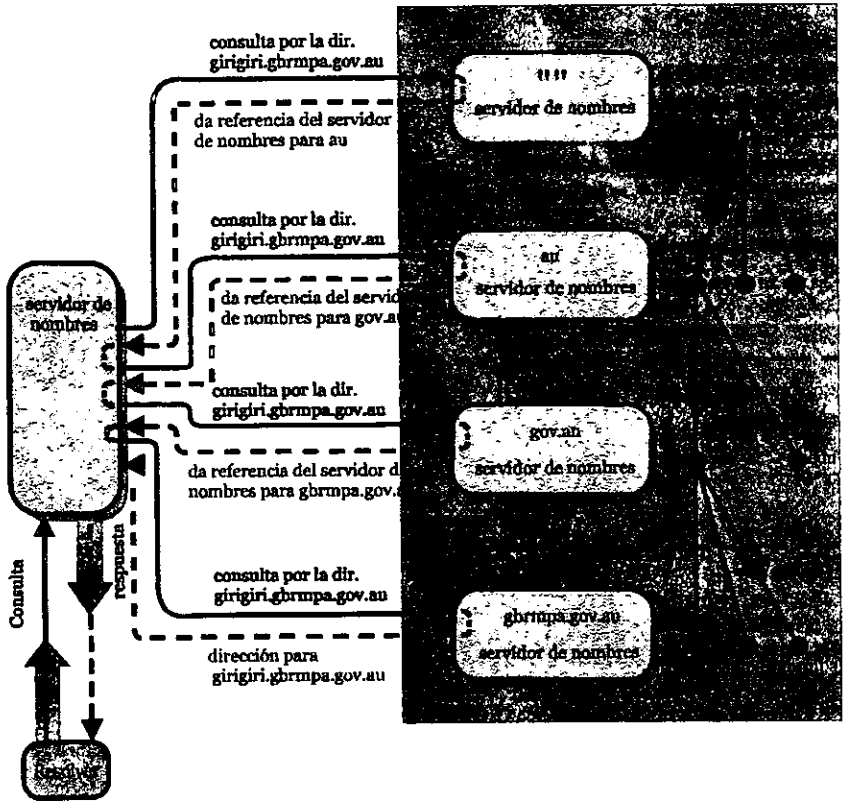
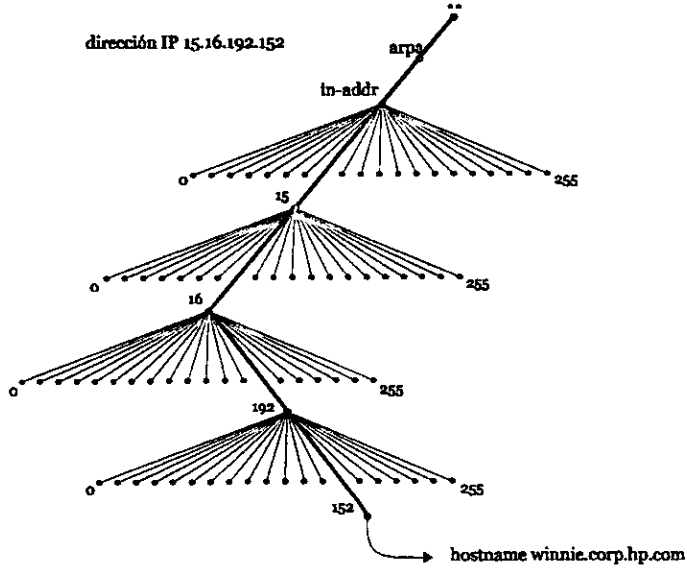


Figura que muestra la resolución para girigiri.gbrmpa.gov.au en Internet

El servidor de nombres local consulta a los servidores de nombres de la raíz por la dirección girigiri.gbrmpa.gov.au, los cuales le dan referencia por el servidor de nombres para el dominio au. Vuelve a preguntar pero ahora al servidor de nombres de au, para lo cual le dan referencia por el servidor de nombres para el dominio gov.au. Éste servidor al ser consultado, da referencia del servidor de nombres para el dominio gbrmpa.gov.au. Finalmente el servidor de nombres local pregunta al servidor de nombres de gbrmpa.gov.au por la dirección, y éste ya recibe la dirección solicitada.

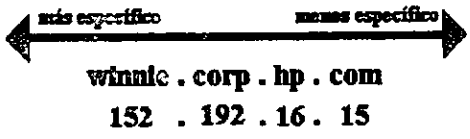
2.4.2 Mapeo entre direcciones IP y nombres

Una de las partes más importantes en la funcionalidad del proceso de resolución es el del mapeo que se realiza entre las direcciones IP y los nombres. El mapeo de dirección-nombre se usa para facilitarle a las personas la lectura e interpretación de las direcciones IP. Cuando se usan tablas de hosts, el mapeo de dirección-nombre es trivial. Esto es porque se requiere llevar a cabo una búsqueda directa y secuencial en las tablas de host por una dirección IP. La búsqueda regresa un nombre oficial de un hosts que se encuentra en la lista de la tabla. En el DNS, el mapeo de dirección-nombre es muy simple. Los datos, incluyendo las direcciones, están ordenadas por nombre en el espacio de dominios. Encontrar una dirección dado un nombre de dominio es relativamente fácil. Pero encontrar el nombre de dominio por mapeo y regresar la dirección IP requiere de una exhaustiva búsqueda en cada nombre de dominio en el árbol.
Actualmente hay una mejor solución para hacer este proceso mas eficiente. En el espacio de nombres de dominio en Internet, a esta porción del espacio se le conoce como el dominio in-addr.arpa.
Los nodos en el dominio in-addr.arpa, son nombres seguidos por números con una estructura similar a la de las direcciones IP.
El dominio in-addr.arpa puede tener hasta 256 subdominios, correspondiendo a cada posible valor del primer octeto de una dirección IP. Cada uno de estos puede tener hasta 256 subdominios más abajo, que corresponde al segundo octeto de una dirección IP. Finalmente, al cuarto nivel, le corresponden los recursos registrados adjuntos al final del octeto dando el nombre completo del dominio del hosts en la red al igual que su dirección IP.



Dominio in-adr.arpa

Se puede observar que cuando se lee el nombre del dominio, la dirección IP aparece al revés desde el nivel más bajo del árbol.
Por ejemplo, si winnie.corp.hp.com tiene la dirección IP 15.16.192.152, el dominio in-addr.arpa correspondiente es 152.192.16.15.in-addr.arpa el cual mapeado al revés se refiere al nombre de dominio winnie.corp.hp.com.
Las direcciones IP son jerárquicas al igual que los nombres de dominio. La diferencia es que las direcciones IP son más específicas de izquierda a derecha, mientras que los nombres de dominio dejan de serlo, como se muestra en la figura.



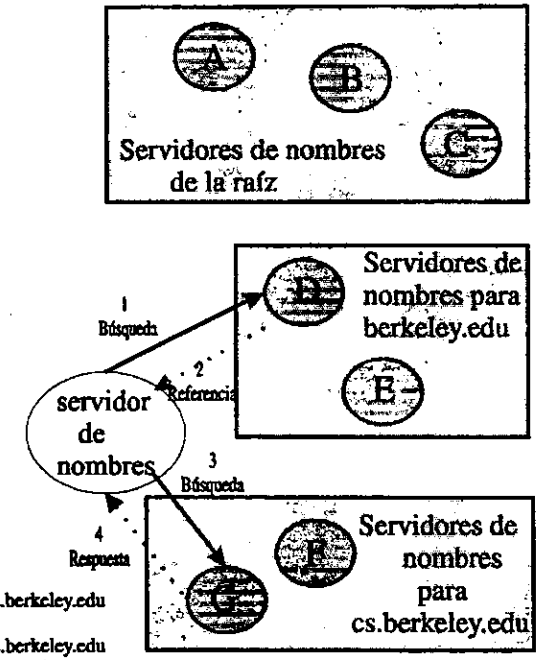
Jerarquización de los nombres y direcciones

Al hacer que el primer octeto de la dirección IP aparezca en lo más alto del árbol brinda al administrador la habilidad de delegar autoridad para los dominios in-addr.arpa, a lo largo de la red. Por ejemplo, el dominio 15.in-addr.arpa, que contiene la información del mapeo inverso, para todos los hosts cuya dirección IP empieza con 15, y que pueden ser delegados al administrador de la red 15. Esto sería imposible si los octetos aparecieron en orden inverso. Si la dirección IP se representara en ese orden, 15.in-addr.arpa se consideraría como un host cuya dirección IP terminaría en 15 por lo que prácticamente el dominio no podría ser delegado.

2.4.3 Caché

Para algunas personas, el proceso de resolución puede parecer muy complicado; pero para otras, es una simple búsqueda en una tabla de hosts. Actualmente, este proceso es muy sencillo. Una de las características que reafirman lo anterior es lo que se conoce como cache.
El procesamiento del servidor de nombres es una búsqueda recursiva que puede enviar muchas o pocas búsquedas para encontrar una solución. Sin embargo, aunque encuentre mucha información sobre el espacio de nombres de dominio, lo seguirá haciendo. En cada momento que se haga referencia a otra lista de servidores de nombres, éste aprenderá que estos servidores de nombres son autoridad para alguna zona, así también aprenderá las direcciones de estos servidores. Y al final del proceso de resolución, cuando encuentre los datos de la búsqueda original, éste podrá guardar los datos para futuras referencias. El cache de los servidores de nombres, ayudará a agilizar las sucesivas búsquedas. En la siguiente resolución del servidor de nombres en la búsqueda de un nombre de dominio, el servidor de nombres ya conocerá algunos datos, por lo que el proceso de búsqueda será

mas corto y por lo tanto más rápido. El servidor de nombres tal vez tenga en cache la respuesta, y en este caso entregará la solución al resolver. Por el contrario, si en el cache no existe la respuesta exactamente, tal vez si se encuentre la identidad de los servidores de nombres que son autoridad de la zona del nombre de dominio que se busca, y así sea capaz de realizar la búsqueda directamente.
Por ejemplo, supongamos que ya se había realizado una búsqueda por el nombre de dominio eecs.berkeley.edu. En este proceso, el caché guardó los nombres y direcciones de los servidores de nombres para los dominios eecs.berkeley,edu y berkeley.edu. Ahora el resolver desea realizar la búsqueda de la dirección para baobab.cs.berkeley.edu, pero el servidor de nombres podrá omitir la búsqueda en los servidores de nombres de la raíz. Reconociendo que el dominio berkeley.edu es antecesor y encierra al dominio baobab.cs.berkeley.edu, por lo tanto, éste conoce todos sus datos, por lo que nuestro servidor de nombres podrá empezar su búsqueda en el servidor de nombres para berkeley.edu, Como se muestra en la figura. Como se puede ver, nuestro servidor de nombres ya había realizado la búsqueda de la dirección para eecs.berkeley.edu, por lo que al momento de recibir otra petición de búsqueda, éste simplemente respondería apropiadamente desde el cache.



1 Búsqueda por baobab.cs.berkeley.edu
2 Referencia de F y G
3 Búsqueda por baobab.cs.berkeley.edu
4 Dirección de baobab.cs.berkeley.edu

A demás de brindar rapidez en la resolución, el caché previene de realizar búsquedas repetitivas a los servidores de nombres de la raíz. Esto significa que nuestros servidores de nombres no dependerán de los de la raíz, y que además los últimos, no sufrirán de consultas innecesarias.

2.4.4 Tiempo de vida (Time to Live)

Los servidores de nombres no pueden mantener los datos en cache por siempre. Si así fuera, los cambios que hubieran en los servidores de nombres que son autoridad nunca alcanzarían al resto de la red.
Los servidores de nombres remotos, simplemente continuarían usando los datos del cache. Consecuentemente, el administrador de la zona que contiene los datos, decide el uso del *time to live*, o TTL para los datos. El *time to live* es la suma del tiempo que cualquier servidor tiene permitido para mantener en cache los datos. Después de este tiempo de vida de caducidad, el servidor de nombres descarta los datos del cache y consigue nuevos datos del servidor de nombres autoridad. Esto también se aplica al cache de datos negativo[8].
Al seleccionar un tiempo de vida para los datos, es necesario hacer un balance entre el desempeño y la consistencia. Un pequeño TTL puede ayudar a asegurar que los datos de los dominios sean consistentes a través de la red, porque los servidores de nombres remotos pueden tomarse mas tiempo y así forzar las consultas al servidor de nombres autoridad con mas frecuencia para obtener los nuevos datos. Así también, esto puede incrementar la carga en el servidor de nombres y alargar el tiempo de resolución de la información en el dominio.
Un TTL grande puede acortar el promedio del tiempo que se toma en resolver la información en el dominio, desde los datos que tiene guardados en el cache. La desventaja es que la información puede ser inconsistente por largos momentos si hay cambios en los datos del servidor de nombres.

2.5 ARCHIVOS DE CONFIGURACIÓN DEL DNS.

Para poder comprender más claramente los siguientes conceptos, en este capítulo se usarán dos servidores de nombres para un dominio ficticio.
El dominio que se usará es para una Universidad de Cine, que estudia todos los aspectos de la industria del cine, buscando diversos caminos para distribuir sus filmes. Uno de sus principales proyectos es la distribución interna, utilizando una red Ethernet como medio de distribución. Después de que se habló con las personas del NIC, se decidió usar el dominio *movie.edu*. El siguiente paso de este proyecto es conectarse a Internet.
La universidad tiene dos Ethernets, las cuales tienen asociadas las redes 192.249.249 y la 192.253.253. Una porción de su tabla de hosts es la siguiente:

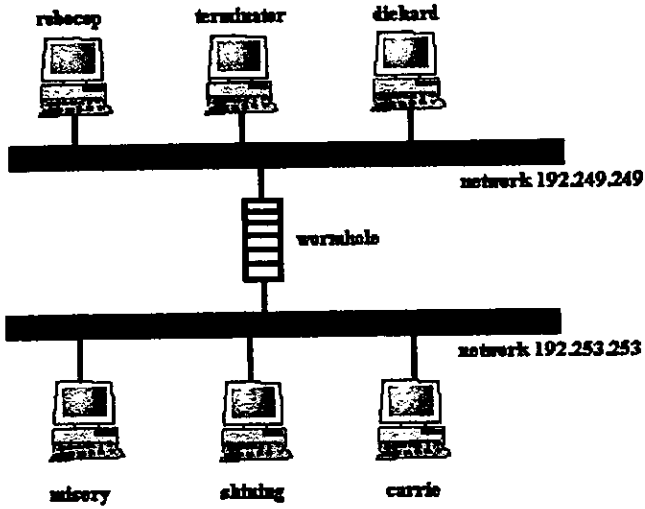
[8] El cache negativo es cuando el servidor de nombres autoridad, responde a una consulta diciendo que el tipo de información de dicha consulta no existe para el nombre de dominio específico.

127.0.0.1	localhost
192.249.249.2	robocop.movie.edu
192.249.249.3	terminator.movie.edu
192.249.249.4	diehard.movie.edu
192.253.253.2	misery.movie.edu
192.253.253.3	shining.movie.edu
192.253.253.4	carrie.movie.edu

ruteador

192.249.249.1	wormhole.movie.edu
192.253.253.1	wormhole.movie.edu

Su red es como la que se muestra en la siguiente gráfica:



El siguiente paso dentro del proceso de la Universidad es pasar los datos de su tabla de hosts a su equivalente en el DNS.

El DNS tiene múltiples archivos. Uno de estos archivos es el mapa de todos los nombres de los hosts y sus direcciones. Otro archivo corresponde al mapa de las direcciones inversas con sus respectivos nombres de hosts.
Al archivo de mapeo de los nombres de hosts a direcciones es conocido como db.DOMAIN. Al archivo de mapeo de direcciones a nombres de dominio es conocido como db.ADDR en donde ADDR es el identificador de la red. A la colección de los archivos db.DOMAIN y los db.ADDR se les conoce como archivos de la base de datos del DNS.
Otro par de archivos es el db.cache y el db.127.0.0. Cada servidor de nombres necesita tenerlo, y éstos son más o menos los mismos para cada servidor.
Todos estos archivos deben estar juntos, en el servidor de nombres se necesita configurar los archivos en el BIND en un archivo que usualmente es llamado /etc/named.boot.
Para inicializar los archivos, es necesaria de una implementación en el servidor de nombres, es este caso el BIND.

2.5.1 Resource Records (RR)

Las entradas en los archivos db son llamadas *DNS resource records.* La búsqueda en el DNS es insensitiva, por lo que se pueden introducir los nombres en la base de datos en mayúsculas, minúsculas o ambas. Pero se recomienda el uso de minúsculas. Los *resource records* necesitan empezar en la primer columna. En el RFC del DNS, los ejemplos presentan a los *resource records* en cierto orden; pero éste no es requerido, por lo que en este trabajo el orden que se presentará es el siguiente:

SOA record
Indica la autoridad para el dominio
NS record
Lista los servidores de nombres para ese dominio
A
Mapa nombre-dirección
CNAME
Nombre canónico (aliases)
PTR
Mapa de dirección-nombre
MX
Correo electrónico
HINFO
Información de los hosts
TXT
Información textual

RP
Persona responsable

El formato estándar de los *resource records* es el que se presenta a continuación, dando una explicación en general de sus componentes.

{nombre} {TTL} Clase Tipo Parámetros de acuerdo al tipo

El primer campo es siempre el nombre del dominio y éste siempre debe iniciar en la primer columna. Para todos los demás RR que se encuentran después, el espacio del nombre puede dejarse en blanco; en este caso, éste toma el valor del RR anterior.
El segundo campo es opcional y corresponde al tiempo de vida, *time to live*. Este campo especifica cuanto tiempo se almacenaran los datos en la base de datos. Si se deja este espacio en blanco el tiempo por default es el que se especificará en el RR *Start Of Authority* (SOA). El tercer campo corresponde a la clase; actualmente solo se soporta una clase, la IN para las direcciones u otra información de Internet. Un soporte limitado esta incluido en la clase HS, en donde se encuentra la información de MIT/Athena "Hesiod".
El cuarto campo corresponde al tipo del *resource record*. El siguiente campo es el que depende del tipo del *resource records* que se haya seleccionado. El caso se conserva en nombres y datos de los campos cuando se carga dentro del servidor de nombres.

Los siguientes caracteres tienen un significado especial dentro de los *resource records*.

"." El punto hace referencia a los dominios de la raíz.
"@" Arroba en el campo de nombre se refiere al actual origen.
"()" Los paréntesis son usados en grupos de datos que ocupan más de una línea. Las terminaciones de línea no son reconocidas dentro de los paréntesis. Esta notación solo trabaja en los RR SOA y no es opcional.
";" Este carácter indica inicio de un comentario.

Los archivos db son fáciles de leer si cuentan con comentarios y líneas en blanco. Los comentarios empiezan con (;) y terminan al final de la línea. El servidor de nombres ignora los comentario y las línea en blanco.

2.5.2 Registros SOA - Start Of Authority

La primer entrada en cada uno de estos archivos es el registro SOA. El registro SOA indica el nombre del servidor y es la mejor fuente de información para los datos dentro del dominio. En el ejemplo, el servidor de nombres es autoridad para el dominio *movie.edu* de acuerdo al registro SOA. El registro SOA es requerido en cada archivo db.DOMAIN y db.ADDR. Solo debe haber un registro SOA en cada archivo db.

{nombre}	{TTL}	Clase	Tipo	Origen	Persona encargada
movie.edu.		IN	SOA	terminator.movie.edu.	al.robocop.movie.edu. (
				1	; Serial
				10800	; Refresh
				3600	; Retry
				604800	; Expire
				86400)	; Minimum

En este ejemplo, el nombre *movie.edu* necesita empezar en la primer columna del archivo. Debemos asegurarnos que el nombre termine con punto.
El IN como ya se mencionó es la clase para Internet. El primer nombre después de SOA (terminator.movie.edu.) es el nombre del servidor primario para estos datos. El segundo nombre (al.robocop.movie.edu.) es la dirección de correo de la persona encargada de los datos en donde @ se cambia por una punto.
El paréntesis permite al registro SOA extenderse mas de una línea.
El número serial es el número de la versión de los datos del archivo y necesita ser un número positivo. Este número necesita incrementarse al hacerse cualquier cambio en los datos. Se puede notar que el uso de la notación "YYYYMMDDNN" puede permitir hacer 100 cambios por día. Pero se puede escoger cualquier notación para trabajar. El *refresh* indica con que frecuencia, en segundos, el servidor de nombres secundario va a estar verificando al servidor de nombres primario para poder actualizar sus datos. El *retry* indica cuanto tiene que esperar el servidor de nombres secundario, en segundos, para volver a procesar una transferencia de zona fallida. El *expire* es el límite máximo, en segundos, que el servidor de nombres secundario usa los datos antes de que expiren para realizar el refresh. El *minimum* es el número por default en segundos que es usado por el *time to live* en los *resource records* cuando no se especifica en los archivos de zona.

2.5.3 Registros NS - Name Server

La siguiente entrada que se agregará a cada archivo es el registro NS, en el cual se listarán los servidores de nombres responsables del dominio, creando delegación y subzonas. Aquí se agregará un registro NS por cada servidor de nombres por dominio. Por lo tanto se tendría lo siguiente:

{nombre}	{TTL}	Clase	Tipo	Parámetros de acuerdo al tipo
movie.edu.		IN	NS	terminator.movie.edu.
movie.edu.		IN	NS	wormhole.movie.edu.

Este registro indica que hay dos servidores de nombres para el dominio movie.edu.
El primer nombre especifica la zona a la que servirá el servidor de nombres que se especifica en el segundo nombre. Cada zona necesita tener por lo menos dos servidores de nombres.

2.5.4 Registros A - Address

El registro A, lista las direcciones. El campo de nombre es el nombre de la máquina y las direcciones son las direcciones IP. Se recomienda tener un registro A por cada dirección de las máquinas.
Este registro hace un mapeo de un nombre a una dirección o varias direcciones, a diferencia de una tabla de hosts, en donde solo se asocia un nombre a una dirección IP. El DNS puede regresar mas de una dirección para un nombre, como puede ser el caso de los ruteadores.
Si la máquina que hace la búsqueda y el servidor de nombres están en la misma red, el servidor de nombres puede localizar en la lista de direcciones la primera que encuentre para tener un mejor desempeño. A esto se le llama *sorteo de direcciones*. Si el sorteo de direcciones no se aplica, las direcciones son robadas en cada búsqueda y así subsecuentemente la lista responderá asignando diferente orden.
Un ejemplo de este registro es el que se presenta a continuación, en donde el wormhole es un ruteador.

{nombre}	{TTL}	Clase	Tipo	Dirección
localhost.movie.edu.		IN	A	127.0.0.1
robocop.movie.edu.		IN	A	192.249.249.2
terminator.movie.edu.		IN	A	192.249.249.3
diehard.movie.edu.		IN	A	192.249.249.4
misery.movie.edu.		IN	A	192.253.253.2
shining.movie.edu.		IN	A	192.253.253.3
carrie.movie.edu.		IN	A	192.253.253.4
wormhole.movie.edu.		IN	A	192.249.249.1
wormhole.movie.edu.		IN	A	192.253.253.1

2.5.5 Registros CNAME - Canonical Name

El registro CNAME relaciona los alias o apodos con el nombre oficial, nombre canónico o nombre del host. Únicamente en este registro se puede asociar con un alias. Todos los otros registros deben estar asociados con el nombre canónico y no con un alias. Cualquier registro RR que incluya un nombre de dominio como su valor, (NS o MX) necesita listar nombres canónicos. Por lo tanto, un alias nunca debe apareces a la derecha del *resource record.*
Los alias son usados cuando para un hosts se desea tener uno o mas nombres asociados.
Cuando un servidor de nombres busca un nombre y encuentra un CNAME, éste reemplaza el nombre por el nombre canónico y busca un nuevo nombre. Por ejemplo, cuando el servidor de nombres busca wh, éste encuentra el registro CNAME apuntando a wormhole, wormhole es buscado, y regresa la dirección.
Como una regla, cuando se tiene un *host multihomed* (cuando se tiene más de una interface de red), se creará un registro A por cada alias apuntando a cada una de las direcciones; así como un registro

CNAME por cada alias común a todas las direcciones, pero estos aliases, son solo para uso del administrador.
Por ejemplo:

```
;
; Hosts  Multihomed
;
wormhole.movie.edu.        IN      A       192.249.249.1
wormhole.movie.edu.        IN      A       192.253.253.1
;
;Aliases
;
bigt.movie.edu.            IN      CNAME   terminator.movie.edu.
dh.movie.edu.              IN      CNAME   diehard.movie.edu.
wh.movie.edu.              IN      CNAME   wormhole.movie.edu.

wh249.movie.edu.           IN      A       192.249.249.1
wh253.movie.edu            IN      A       192.253.253.1
```

2.5.6 Registros PTR - Domain Name Pointer

El registro PTR es el que se encarga de realizar el mapeo de dirección a nombre. El archivo db.192.249.249 mapea de las direcciones a los nombres de los hosts para la red 192.249.249. Este de be ser un registro por cada host conectado a la red.
Aquí se muestran los datos creados para la red 192.249.249:

```
1.249.249.192.in-addr.arpa.  IN   PTR   wormhole.movie.edu.
2.249.249.192.in-addr.arpa.  IN   PTR   robocop.movie.edu.
3.249.249.192.in-addr.arpa.  IN   PTR   terminator.movie.edu.
4.249.249.192.in-addr.arpa.  IN   PTR   diehard.movie.edu.
```

En este ejemplo, cabe mencionar algunos puntos. En primer lugar, las direcciones necesitan apuntar a únicamente un nombre, el nombre canónico. Así la dirección 192.249.249.1 mapea a wormhole y no a wh249. Se pueden crear dos registros PTR, uno para wormhole y otro para wh249, pero la mayoría de los sistemas, no están preparados para ver más de un nombre apuntando a una dirección. Segundo, aunque wormhole tenga dos direcciones, aquí únicamente se podrá ver una de ellas; esto es porque este archivo muestra solo las conexiones directas a la red 192.249.249, y wormhole tiene solo una conexión a ella.

2.5.7 Registros MX - Mail Exchanger

El registro MX, es usado para especificar los hosts que están configurados para recibir o enviar correo electrónico para su nombre de dominio. Un host puede procesar el correo o reenviarlo a otro nombre de dominio. Procesarlo consiste en entregar el correo a una dirección en particular o bien dirigirlo a otro transporte de correo, como UUCP. Reenviarlo significa transmitirlo a un destino final o a otro mail exchanger vía SMTP.
El registro MX tiene un parámetro extra entre el nombre de dominio y el mail exchanger; el valor de preferencia. Éste valor es un número de 16 bits (entre 0 y 65535) que indica la prioridad del mail exchanger. Por ejemplo, el registro MX:

```
peets.mpk.ca.us.    IN    MX    10    relay.hp.com.
```

indica que relay.hp.com. es mail exchanger para peets.mpk.ca.us. con un valor de preferencia de 10. Tomándolo ya en conjunto, el valor de preferencia de un mail exchanger para un host, se refiere al orden en el que el buscador los podrá usar. El valor de preferencia por sí mismo no importa, sólo si se relaciona con los valores de otros mail exchangers. Como por ejemplo:

```
plange.puntacana.dr.  IN    MX    1     listo.puntacana.dr.
plange.puntacana.dr.  IN    MX    2     hep.puntacana.dr.
```

es exactamente lo mismo que tener:

```
plange.puntacana.dr.  IN    MX    50    listo.puntacana.dr.
plange.puntacana.dr.  IN    MX    100   hep.puntacana.dr.
```

Los servidores de correo entregarán primero el mail exchanger a quien tenga el valor de preferencia mas bajo. Por lo tanto, el mejor mail exchanger es el que tenga el valor de preferencia igual a 0.
Si la entrega del correo al mail exchanger de mayor preferencia fracasa, el servidor puede intentar entregarlo al mail exchanger que tenga menor preferencia (esto significa a un mail exchanger que tenga un valor de preferencia más alto).
Más de un mail exchanger pueden tener el mismo valor de preferencia. Esto permitirá al servidor tener mas opciones de envío además del primero. Así, de esta manera, también agotará las opciones que tengan el mismo valor de preferencia antes de pasar al siguiente nivel de preferencia. Por ejemplo, el registro MX para ora.com podría ser:

```
ora.com.    IN    MX    0     ora.ora.com.
ora.com.    IN    MX    10    ruby.ora.com.
ora.com.    IN    MX    10    opal.ora.com.
```

Interpretando estos datos ya en conjunto, los registros MX dirigirán al servidor para que éste pueda entregar el correo a ora.com, enviándolo a:

1.- ora.com. primeramente
2.- es caso de que fracase, después lo enviará a ruby.com. u cpal.ora.com para finalizar, pero no a ambos al mismo tiempo; primero a uno y si vuelve a fracasa, pasará con el otro.

Solo si fracasa en su primera opción, pasará a la siguiente. Si entrega con éxito desde un principio, aquí se detendrá.

2.5.8 Registros HINFO - Host Information

El registro HINFO es para datos específicos de los hosts. Este lista el hardware y sistema operativo que están corriendo en la lista de hosts. Se debe tener un registro HINFO por cada host, aunque por razones de seguridad, la mayoría de los dominios no tienen registros HINFO.

{nombre}	{TTL}	Clase	Tipo	Hardware	OS
		IN	HINFO	VAX-11/780	UNIX

2.5.9 Registros TXT - Text

Un registro TXT contiene datos textuales de cualquier tipo. La sintaxis del texto depende del dominio en donde se encuentre. Muchos sistemas usan este registro para presentar los datos en un formato estilizado.

{nombre}	{TTL}	Clase	Tipo	Cadena
Munnary.OZ.AU.		IN	TXT	"foo"

2.5.10 Registros RP - Responsible Person

El registro RP identifica el nombre o grupo de nombres de las personas responsables del host. Ofrece la capacidad de identificar la identidad del responsable para el host en particular. Cuando el host se encuentre deshabilitado o que este funcionando incorrectamente, se puede contactar a las personas que se encuentren registradas aquí, las cuales pueden ser capaces de resolver el problema.
El campo de buzón de correo, es el nombre de dominio que especifica el buzón de correo para la(s) persona(s) responsable(s). Su formato es igual al que se usa en el registro SOA, en donde @ de la cuenta de correo se sustituye por un punto.
El campo de TXT es el nombre del dominio para el cual el registro TXT existe. En el ejemplo, sysadmins.berkeley.edu. es el nombre del registro TXT del cual se piensa contiene algún texto con nombres y número telefónicos.
El registro PR es aún de carácter experimental, ya que no todos lo servidores de nombres lo reconocen aún.

{nombre}	{TTL}	Clase	Tipo	Buzón de correo	TXT
franklin		IN	RP	ben.franklin.berkeley.edu.	sysadmins.berkeley.edu.

2.5.11 Estructura final de los archivos

Ahora que se han explicado los resource records (RR), de los archivos db, se considera necesario presentar la estructura final de dichos archivos con todos los datos.

Contenido del archivo db.movie:

```
movie.edu.          IN    SOA   terminator.movie.edu.     al.robocop.movie.edu. (
                                        1          ; Serial
                                        10800      ; Refresh
                                        3600       ; Retry
                                        604800     ; Expire
                                        86400 )    ; Minimum

;
;Servidores de Nombres
;
movie.edu.                  IN          NS          terminator.movie.edu.
movie.edu.                  IN          NS          wormhole.movie.edu.

;
;Direcciones para los nombres canónicos
;
localhost.movie.edu.            IN          A       127.0.0.1
robocop.movie.edu.              IN          A       192.249.249.2
terminator.movie.edu.           IN          A       192.249.249.3
diehard.movie.edu.              IN          A       192.249.249.4
misery.movie.edu.               IN          A       192.253.253.2
shining.movie.edu.              IN          A       192.253.253.3
carrie.movie.edu.               IN          A       192.253.253.4

wormhole.movie.edu.             IN          A       192.249.249.1
wormhole.movie.edu.             IN          A       192.253.253.1

;
;Aliases
;
bigt.movie.edu.                 IN          CNAME   terminator.movie.edu.
dh.movie.edu.                   IN          CNAME   diehard.movie.edu.
wh.movie.edu.                   IN          CNAME   wormhole.movie.edu.

;
```

```
; Nombres especiales para las interfaces
;
wh249.movie.edu.          IN        A          192.249.249.1
wh253.movie.edu           IN        A          192.253.253.1
```

Contenido del archivo db.192.249.249:

```
249.249.192.in-addr.arpa.  IN   SOA  terminator.movie.edu.   al.robocop.movie.edu. (
                                     1          ; Serial
                                     10800      ; Refresh
                                     3600       ; Retry
                                     604800     ; Expire
                                     86400 )    ; Minimum

;
;Servidores de Nombres
;
249.249.192.in-addr.arpa.   IN          NS          terminator.movie.edu.
249.249.192.in-addr.arpa.   IN          NS          wormhole.movie.edu.

;
;Direcciones para los nombres canónicos
;
1.249.249.192.in-addr.arpa.  IN   PTR   wormhole.movie.edu.
2.249.249.192.in-addr.arpa.  IN   PTR   robocop.movie.edu.
3.249.249.192.in-addr.arpa.  IN   PTR   terminator.movie.edu.
4.249.249.192.in-addr.arpa.  IN   PTR   diehard.movie.edu.
```

Contenido del archivo db.192.253.253:

```
253.253.192.in-addr.arpa.  IN   SOA  terminator.movie.edu.   al.robocop.movie.edu. (
                                     1          ; Serial
                                     10800      ; Refresh
                                     3600       ; Retry
                                     604800     ; Expire
                                     86400 )    ; Minimum

;
;Servidores de Nombres
;
253.253.192.in-addr.arpa.   IN          NS          terminator.movie.edu.
253.253.192.in-addr.arpa.   IN          NS          wormhole.movie.edu.
```

```
;
;Direcciones para los nombres canónicos
;
1.253. 253.192.in-addr.arpa. IN    PTR   wormhole.movie.edu.
2. 253. 253.192.in-addr.arpa. IN   PTR   misery.movie.edu.
3. 253. 253.192.in-addr.arpa. IN   PTR   shining.movie.edu.
4. 253. 253.192.in-addr.arpa. IN   PTR   carrie.movie.edu.
```

2.5.12 Archivo de respaldo

Un servidor de nombres, necesita de un archivo adicional en el cual se pueda hacer el respaldo, este archivo es el db.ADDR, la dirección especial del host se utiliza para dirigir el tráfico a él mismo. Esta red es casi siempre la 127.0.0 así como la dirección del host que es la 127.0.0.1. Por esta razón el nombre de este archivo es db.127.0.0.

Contenido del archivo db.127.0.0

```
0.0.127.in-addr.arpa.  IN SOA terminator.movie.edu.  al.robocop.movie.edu. (
                              1          ; Serial
                              10800      ; Refresh after 3 hours
                              3600       ; Retry after 1 hour
                              604800     ; Expire after 1 week
                              86400      ; Minimum TTL of 1 day

0.0.127.in-addr.arpa.  IN NS  terminator.movie.edu.
0.0.127.in-addr.arpa.  IN NS  wormhole.movie.edu.

1.0.0.127.in-addr.arpa.  IN   PTR localhost.
```

El servidor de nombres puede trabajar sin este archivo. Sin embargo, la búsqueda a la dirección 127.0.0.1, podría fallar porque el servidor de nombres contactado no fue configurado para hacer el mapeo entre el nombre y la dirección 127.0.0.1, o porque los servidores de nombres de la raíz contactados, imaginan proveer una respuesta para el localhost.

2.5.13 Archivo root.cache

Además de la información local, el servidor de nombres necesita conocer la localización de los servidores de nombres que atienden a los dominios de la raíz. Esta información se puede obtener a través de Internet haciendo un ftp al *host ftp.rs.internic.net* (198.41.0.5). En el ftp se usará el usuario *anonymous* y se podrá obtener el archivo *named.root* desde el directorio *domain.*

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache . <file>"
;       configuration file of BIND domain name servers).
;
;       This file in made available by InterNIC registration services
;       under anonymous FTP as
;               file                    /domain/named.root
;               on server               FTP.RS.INTERNIC.NET
;               -OR- under Gopher at    RS.INTERNIC.NET
;               under menu              InterNIC Registration Services (NSI)
;                   submenu             InterNIC Registration Archives
;               file                    named.root
;
;               last update:    Sep 1, 1995
;               related version of root zone:       1995090100
;
;
;       formely NS.INTERNIC.NET
;
.                        3600000      IN    NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000            A     198.41.0.4
;
;       formely NS1.ISI.EDU
;
.                        3600000            NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000            A     128.9.0.107
;
;       formely C.PSI.NET
;
.                        3600000            NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000            A     192.33.4.12
;
;       formely TERP.UMD.EDU
;
.                        3600000            NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000            A     128.8.10.90
;
;       formely NS.NASA.GOV
;
.                        3600000            NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000            A     192.203.230.10
```

```
;
;       formely NS.ISC.ORG
;
.                       3600000         NS      F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000         A       39.13.229.241
;
;       formely NS.NIC.DDN.MIL
;
.                       3600000         NS      G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000         A       192.112.36.4
;
;       formely AOS.ARL.ARMY.MIL
;
.                       3600000         NS      H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000         A       128.63.2.53
;
;       formely NIC.NORDU.NET
;
.                       3600000         NS      I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000         A       192.36.148.17
; End of File
```

El nombre de dominio "." se refiere a los dominios de la raíz. Si los servidores de nombres de los dominios de la raíz, sufren alguna modificación, esto no significa que ésta lista se actualizará, por lo que se tiene que obtener nuevamente el archivo named.root.
Como hace este archivo para guardar los datos? Como administrador de la red, necesita guardar los datos. Algunas versiones de BIND, pueden actualizar este archivo periódicamente. Algunas veces los cambios al archivo db.cache son enviados a el bind o a las listas de correo.
En versiones anteriores de este archivo, el número usado era el 99999999. Desde que este archivo fue el caché de los datos, el servidor de nombres necesitó conocer cuanto tiempo tenía para realizar los respaldos. El 99999999 significaba que tenía mucho tiempo. Los servidores de nombres de la raíz, no podían mantenerse activos por mucho tiempo. Desde que los servidores de nombres guardan los datos en un lugar especial, y que no descartan si este tiempo terminó, el TTL es innecesario. Esto no significa que perjudique el tener el 3600000, haciéndose mas interesante para el BIND cuando se traspasa la responsabilidad al siguiente servidor de nombres.

2.6 INICIALIZACIÓN DE LOS ARCHIVOS

Ahora que los archivos db han sido creados, al servidor de nombres se le tiene que indicar la manera en que debe leer cada uno de éstos archivos.
Para BIND, el mecanismo para apuntar a estos archivos es por medio del archivo boot.

Aunque el archivo boot es esencial para BIND, éste no está definido en los RFCs del DNS.
Usualmente el archivo boot contiene una línea en la que se indica el directorio en donde se encuentran los archivos. El servidor de nombres cambia a este directorio antes de leer los archivos. Esto permite al sistema de archivos, ser relativo al actual directorio, en vez de hacerlo desde la raíz.
Aquí se muestra como debe aparecer esta línea de directorio:

directory /usr/local/named

En el servidor primario, el archivo contiene una línea por cada archivo que debe leer. Esta línea contiene tres campos: la palabra primary, iniciando en la primera columna, el dominio del servidor para donde es autoridad, y el nombre del archivo.

primary	movie.edu	db.movie
primary	249.249.192.in-addr.arpa	db.192.249.249
primary	253.253.192.in-addr.arpa	db.192.253.253
primary	0.0.127.in-addr.arpa	db.127.0.0

Aquí es en donde el archivo boot lee el archivo caché.

cache	.	db.cache

Este archivo no contiene los datos en general del caché, únicamente contiene indicios de los servidores de nombres de la raíz.

Por default, BIND espera que el archivo boot tenga por nombre /etc/named.boot, pero éste se puede cambiar con un comando en la línea de opción.
Los archivos db para el ejemplo que hemos estado utilizando, se encuentran en el directorio /urs/local/named. El nombre del directorio que utilice no importa, pero evite colocarlo en el sistema de archivos de la raíz o en algún sistema de archivos que tenga poco espacio.
A continuación se muestra completo el archivo /etc/named.boot:

directory /usr/local/named

primary	movie.edu	db.movie
primary	249.249.192.in-addr.arpa	db.192.249.249
primary	253.253.192.in-addr.arpa	db.192.253.253
primary	0.0.127.in-addr.arpa	db.127.0.0
cache	.	db.cache

2.7 INICIALIZAR EL SERVIDOR DE NOMBRES

Ahora que ya se crearon los archivos de la base de datos del DNS, esta todo listo para inicializar el servidor de nombres. Antes de que echemos a andar el servidor, debemos estar seguros de que el demonio syslog este corriendo. Si el servidor de nombres detecta un error, enviará un mensaje.
En sistema BSD, el demonio puede inicializarse en /etc o bien en algunos otros lugares como son /usr/etc/in.named o en /usr/sbin/in.named.
Para inicializar el servidor, es necesario convertirse en superusuario o bien en root, como es también conocido. El servidor de nombres opera en un puerto reservado que requiere los privilegios con los que cuenta el superusuario.
El servidor no requiere ser root para realizar cualquier otra cosa. Al inicializar el servidor desde la línea de comandos por primera vez, es necesario verificar que este corriendo correctamente.
El siguiente comando sirve para inicializar el servidor. En el dominio movie.edu, se correrá el comando en el host terminator.

/etc/named

Este comando asume que el archivo boot es el /etc/named.boot. En caso de tener como archivo boot cualquier otro archivo, es necesario indicárselo al servidor usando el comando -h en la línea de comandos.

/etc/named -h bootfile

La primera cosa, después de haber inicializado el servidor, es verificar el archivo syslog para poder verificar los mensajes de error. Si no se está familiarizado con el syslog, es recomendable verificar el manual syslog.conf, en donde se muestra la configuración del archivo syslog; o bien el manual de syslog, para verificar la descripción del demonio syslog.
En el servidor de nombres el log de mensajes de un demonio bajo el nombre de named.
Estos archivos los podemos encontrar en/etc/syslog.conf y para verificar si hubo errores, es con el comando
grep daemon /etc/syslog.conf
o
grep named /var/adm/messages

En caso de que haya habido algún error, y que éste se corrigió, es necesario indicarle al servidor de nombres, para que vuelva a reinicializar el proceso.
Esto es con el comando:

kill -HUP

2.8 BIND

El Berkeley Internet Name Domain (BIND) es por mucho la implementación mas popular del DNS hasta ahora.
BIND consiste de un servidor (o demonio) llamado named y de librerías llamadas resolver. Un servidor de nombres es un servicio de red que brinda a los clientes los nombres de los recursos u objetos así como compartirlos con otros objetos en la red.
Esto en efecto, es una distribución de sistemas de bases de datos entre ordenadores conectados a la red. El servidor BIND corre en *background* sirviendo a las búsquedas a través de un puerto que es bien conocido. El puerto estándar para UDP y TCP se especifica en /etc/services. El *resolver* es un grupo de rutinas que reside en el sistema de librerías de C para proveer las interfaces de los programas que hacen uso del acceso a los servicios de nombres de dominio.
BIND es totalmente integrado dentro de los programas BSD[9] para su uso en almacenamiento y recopilación de nombres de host y sus direcciones.

[9] Abreviatura de Berkeley Software Distribution [Distribución de software de Berkeley]. Derivado del sistema operativo UNIX, desarrollado en la Universidad de California, en Berkeley, California. Las adiciones de la BSD al sistema operativo UNIX incluyen el apoyo a la memoria virtual, el apoyo a las redes, la comunicación entre procesos, el apoyo para periféricos adicionales, así como las mejoras para el sistema de archivos y de seguridad.

CAPITULO 3 "HERRAMIENTAS DE BÚSQUEDA"

En este capítulo se analizarán dos de las herramientas más utilizadas para la búsqueda de información en los servidores de nombres. Estas dos herramientas son el nslookup y el dig. Con cualquiera de éstas dos herramientas, se puede identificar el nombre de un dominio, así como su respectiva dirección IP, además de los datos relacionados con cualquiera de los resource records (RR) relacionados con este nombre de dominio.
También nos ayudan a resolver problemas que se lleguen a presentar en cualquier servidor de nombres.
En este capítulo se abundará en el estudio de nslookup, ya que es la herramienta que se utiliza para consultar los cuatro servidores de nombres de RedUNAM. Por este mismo motivo solo se dará una breve explicación del funcionamiento de Dig.

3.1 NSLOOKUP

3.1.1 Características

Para facilitar el proceso de resolución de problemas, es necesario contar con una herramienta especial para poder hacer consultas a los servidores de nombres. Una de estas herramientas es el nslookup. Esta herramienta es distribuida con BIND y con muchos otros sistemas.
Esta herramienta nos proporciona la facilidad de consultar a nuestro propio servidor de nombres, o a otros.
Nslookup utiliza sus propias rutinas para realizar las búsquedas o consultar a los servidores de nombres, pero éstas se basan en los códigos de las rutinas de los resolver.
Consecuentemente, el comportamiento de nslookup es muy similar al comportamiento de un resolver, pero con ligeras diferencias.
En lo que concierne a la emulación del comportamiento de un servidor de nombres, nslookup permite realizar consultas a otros servidores con el mismo paquete de consulta que el servidor de nombres utiliza, pero el esquema de retransmisión es muy diferente; aunque como un servidor de nombres, puede copiar los datos de la zona.

Múltiples servidores

Otra diferencia, es que nslookup solo puede consultar a un servidor de nombres a la vez, lo contrario de un resolver. El resolver hace uso de cada entrada de servidores de nombres que se enlistan en el resolv.conf. Si en este archivo existieran dos líneas de servidores de nombres, el resolver trataría con el primer servidor de nombres, después con el segundo, después con el primero, y así sucesivamente hasta que reciba respuesta o abandone la búsqueda. El resolver hace esto en cada consulta. Por otro lado, el nslookup tratará con el primer servidor de nombres que aparezca en el resolv.conf, aguardará y reintentará, hasta que finalmente se le indique que abandone al primer servidor e intente con otro. Una vez que haya conseguido respuesta, buscará en éste servidor y no tratará con ningún otro.

Esta característica del nslookup, de consultar a un solo servidor de nombres a la vez, es con la finalidad de que al surgir un problema, se nos facilite la búsqueda de la solución al reducir al mínimo las variables y así tener una mejor visión de dicho problema.

Búsqueda de dominios

El nslookup implementa la lista de búsqueda tal como el resolver lo hace. El servidor de nombres no implementa las listas de búsqueda, por lo tanto, para actuar como un servidor de nombres, nslookup, buscará que la función esté con la opción *off*, como se verá más adelante.

Transferencia de zona

El nslookup puede realizar transferencia de zonas tal como un servidor de nombres; pero a diferencia del servidor, el nslookup no verifica el número serial del registro SOA antes de obtener los datos de la zona, éste proceso se tiene que llevar a cabo manualmente si se desea.
Nslookup filtra los datos de la zona por default, y solo muestra las direcciones y los servidores de nombres de los *resource records* (RR) aunque si pueda procesar todos los datos de la zona. A pesar de esto, se puede hacer que nslookup muestre todos los datos de dicha zona.

3.1.2 Versión Interactiva o No Interactiva de nslookup

Como primer paso en el manejo de nslookup, es necesario saber como entrar y como salir de él. Esta herramienta de búsqueda, puede correr en modo interactivo o no interactivo (por medio de la línea de comandos). Si solo se desea observar una parte de los datos, se debe utilizar la forma no interactiva. O bien si se planea hacer una búsqueda de manera mas exhaustiva, como lo es cambiar de servidores, o de opciones, es recomendable utilizar el método interactivo.

Para iniciar con una sesión interactiva, se tecleará:

% ***nslookup***
Default Server: terminator.movie.edu
Address: 0.0.0.0

>^*D* (control D)

Si desea ayuda, teclee ? o *help*. Cuando desee salirse, teclee ^D (control D). Si desea salirse de nslookup interrumpiéndolo, hágalo tecleando ^C (o cualquier carácter de interrupción). Nslookup recibe la señal de interrupción, detiene cualquier proceso que este realizando y presentará nuevamente el prompt >.
Para una búsqueda no interactiva, incluya el nombre que esta buscando en la línea de comando:

% *nslookup carrie*
Server: terminator.movie.edu
Address: 0.0.0.0

Name: carrie.movie.edu
Address: 192.253.253.4

3.1.3 Cambio de opciones

Nslookup tiene un conjunto propio de opciones. Todas estas opciones se pueden cambiar.

% *nslookup*
Default Server: bladerunner.fx.movie.edu
Address: 0.0.0.0
> *set all*
Default Server: bladerunner.fx.movie.edu
Address: 0.0.0.0

Set options:

nodebug	defname	search	recurse
novc	noignoretc	port=53	
querytype=A	class=IN	timeout=5	retry=4
root=a.root-servers.net.			
domain=fx.movie.edu			
srchlist=fx.movie.edu			

> ^*D*

El servidor de nombres por default es bladerunner.fx.movie.edu. Esto significa que cada búsqueda lanzada por nslookup será enviada a bladerunner. La dirección 0.0.0.0 significa "este host". Cuando nslookup usa la dirección 0.0.0.0 o la 127.0.0.1 se refiere a este servidor, o sea, que esta utilizando el servidor de nombres del sistema local, en este caso bladerunner.
Las opciones son de dos formas: *Boolean* o *value*. Ellas tienen la propiedad de ser, ya sea "*on*" u "*off*".
¿Como saber cuando la opción *Boolean* es *on* u *off*? La opción es *off* cuando no precede el nombre de la opción. *Nodebug* significa que *debugging* está apagado (*off*).
El modo de poder cambiar el valor de la opción *boolean*, depende de si se esta utilizando el nslookup interactivo o no. En una sesión interactiva, se puede cambiar la opción con el comando *set*, como por ejemplo *set debug* o *set domain=classics.movie.edu*.
Desde la línea de comando, se omite la palabra *set* y se precede la opción con un guión, como en *nslookup -debug* o *nslookup -domain=classics.movie.edu*. Las opciones se pueden abreviar o colocar

de una forma más corta como por ejemplo: *nodeb* para *nodebug* o la opción *querytype* puede ser llamada simplemente como *type*.
A continuación se presenta una breve explicación de cada una de las opciones:

[no] debug
El debug por default tiene el valor de *off*. Si éste se cambia a *on*, el servidor de nombres mostrará los tiempos de vida y desplegará tanto los paquetes que se envían como los de respuesta. (Abreviación=[no]deb)

[no] defname
Por default, nslookup agrega al nombre de dominio por default a los nombres que no cuentan con un punto al final. Antes de buscar la lista existente, el resolver de BIND podría agregar el dominio por default a los nombres sin un punto. Nslookup puede implementar la prebúsqueda de la lista de comportamientos (con *search* en *off* y *defname* en *on*), o se puede implementar la búsqueda de la lista de comportamiento (con *search* en *on*). (Abreviación=[no]def)

[no] search
La opción *search* es una réplica de la opción del nombre de dominio por default (*defname*). En otras palabras, *defname* únicamente se aplica si *search* se encuentra en *off*. Con defname, se hace una búsqueda de cada nombre en los dominios padres del actual dominio. Por default, nslookup agrega el dominio en la lista de búsqueda (*srchlist*) a los nombres que no terminan en punto.

[no] recurse
Nslookup pide servicio recursivo por default. Éste comando indica al servidor de nombres que consulte a otros servidores si él no cuenta con la información requerida. (Abreviación=[no]rec)

[no] vc
Por default, nslookup hace las consultas usando paquetes de UDP[10] en vez de hacerlo sobre circuitos virtuales (TCP). En la mayoría de los resolvers de BIND las consultas se hacen con UDP, por lo que el comportamiento de nslookup abarca el de los resolvers. Si el resolver puede ser instruido para usar TCP, también se puede realizar en nslookup. (Abreviación=[no]v)

[no] ignorect
Por default, nslookup no ignora los paquetes truncados. Si un paquete es recibido con el bit indicando "truncado", indicando que el servidor de nombres no pudo adaptar toda la información importante en el paquete de respuesta de UDP, nslookup no lo ignora; él regresa la consulta usando una conexión TCP en vez de UDP. Por lo que nuevamente se abarca el comportamiento del resolver de BIND. La razón por la que la respuesta a la consulta usa una conexión TCP es porque la respuesta

[10] Abreviatura de User Datagram Protocol [Protocolo de datagrama de usuario]. Protocolo de nivel de transporte utilizado en el conjunto de protocolos de control de transmisión/Protocolo de Internet o TCP/IP.

de TCP puede ser lo doble de larga que una respuesta de UDP. La respuesta de TCP puede utilizar mucho mas tiempo que una de UDP (una conexión TCP puede cargar muchos mas datos que un simple paquete UDP), pero los buffers de BIND usados por TCP son simplemente el doble de largo que los buffers de UDP. (Abreviación=[no]ig)

port=53
El servicio del DNS se hace por medio del puerto 53. Se puede inicializar el servidor de nombres desde otro puerto, por lo que nslookup también se puede dirigir para que utilice ese mismo puerto.

querytype= *valor*
Por default, nslookup solo revisa los resource récords correspondientes al tipo A (address). Si se teclea una dirección IP (y el query type de nslookup es A o PTR), entonces nslookup puede invertir la dirección, agregando in-addr.arpa, y mostrar los datos de PTR.
Los valores que puede tomar son (A, CNAME, HINFO, MX, NS, PTR, SOA, TXT). (Abreviación=q)

class=IN
La única clase que reconoce es Internet. (Abreviación=cl)

timeout=5
Si el servidor de nombres no responde en 5 minutos, nslookup reenvía la consulta y doblega el tiempo (a 10, después a 20, hasta 40 segundos). El resolver de BIND usa el mismo timeout cuando consulta a un solo servidor de nombres. Este número se puede cambiar. (Abreviación=t)

retry=4
La consulta la envía cuatro veces antes de abandonarla. Después de cada retry, el valor del timeout se dobla. Hasta que se reconozca el comportamiento del resolver BIND. (Abreviación=ret)

root= *host*.
Cambia el nombre del host del servidor de nombres. Este es un comando muy conveniente llamado raíz, que se encarga de conectar el servidor a los servidores de nombres de la raíz. Ejecutando el comando root desde la versión moderna de nslookup, es lo equivalente a ejecutar *server a.root-servers.net*. En versiones anteriores se usaba *nic.addn.mil* o bien *sri-nic.arpa* como los servidores de nombres de la raíz por default. Se puede cambiar el servidor de la raíz por default con *set root=server*. (Abreviación=ro)

domain=*name*
Cambia el nombre del dominio que se encuentra por default. (Abreviación=do)

srchlist=fx.movie.edu
Si search está en on, aparecerán los dominios que se agregan a los nombres que no finalizan en un punto. Los dominios son listados en el orden correspondiente, separados por un slash (/).(Abreviación=srchl)

3.1.4 El archivo .nslookuprc

Se puede dar de alta una nueva opción por default en el archivo nslookuprc. El nslookup revisará el archivo en el directorio *home* cuando éste inicialice, ya sea de modo interactivo o no interactivo. El archivo nslookuprc puede contener cualquier comando set, uno por línea. Esto se recomienda cuando se esta manejando una versión anterior de nslookup en donde sigue pensando que sri-nic.arpa es un servidor de nombres de la raíz. Se puede poner por default un verdadero servidor de nombres de la raíz en el archivo .nslookuprc de la siguiente manera:

set root=a.root-servers.net.

3.1.5 Preguntas más comunes

Buscando diferentes tipos de datos.

Por default, nslookup busca las direcciones de los nombres, o los nombres de las direcciones.
Se puede observar cualquier tipo de datos, cambiando los *querytype* como se muestra en el siguiente ejemplo:

```
% nslookup
Default Server: terminator.movie.edu
Addess: 0.0.0.0

> misery                          Busca una dirección
Server:         terminator.movie.edu
Address:        0.0.0.0

Name:           misery.movie.edu
Address:        192.253.253.2

> 192.253.253.2                   Busca un nombre
Server:         terminator.movie.edu
Address:        0.0.0.0

Name:           misery.movie.edu
Address:        192.253.253.2
```

> set q=mx Busca datos del tipo MX
> wormhole
Server: terminator.movie.edu
Address: 0.0.0.0

wormhole.movie.edu preference=10, mail exchanger = wormhole.movie.edu
wormhole.movie.edu internet address= 192.249.249.1
wormhole.movie.edu internet address= 192.253.253.1

> set q=any Busca datos de cualquier tipo

> diehard
Server: terminator.movie.edu
Address: 0.0.0.0

diehard.movie.edu internet address= 192.249.249.4
diehard.movie.edu preference = 10, mail exchanger = diehard..movie.edu
diehard.movie.edu internte address = 192.249.249.4

Estos son solo algunos ejemplos de los diversos tipos de datos que se pueden observar por medio del nslookup.

Versión Autoritaria, respuesta No Autoritaria

La primera vez que se hace una búsqueda remota de un nombre, la respuesta es autoritaria, pero en las siguientes búsquedas hacia el mismo nombre, la respuesta es no autoritaria.
Esto se puede ver en el siguiente ejemplo:

% nslookup
Default Server: relay.hp.com
Addess: 15.255.152.2

> slate.mines.colorado.edu.
Server: relay.hp.com
Address: 15.255.152.2

Name: slate.mines.colorado.edu
Address: 138.67.1.3

> slate.mines.colorado.edu.
Server: relay.hp.com
Address: 15.255.152.2

Non-authoritative answer:
Name: slate.mines.colorado.edu
Address: 138.67.1.3

Lo que esta pasando en el primer momento que el servidor de nombres local busca por *slate*, es que él contacta al servidor de nombres para mines.colorado.edu, y el servidor para mines.colorado.edu envía una respuesta autoritaria. El servidor de nombres en efecto, pasa directamente la respuesta al respaldo de nslookup. Esto es el cache de respuestas. La segunda vez que se busque *slate*, el servidor de nombres contestara con lo que guardó en el caché, sin tener que contactar nuevamente al servidor, por lo que el resultado es una respuesta no autoritaria.

Conexión de servidores

Algunas veces tendremos que conectarnos a otro servidor de nombres directamente, cuando, por ejemplo, se piensa que éste esta funcionando incorrectamente. En nslookup podemos conectarnos a otro servidor por medio de los comandos *server* y *lserver*. La diferencia entre server y lserver es que *lserver* consulta en el servidor local para conseguir la dirección del servidor al que se desea contactar; al usar *server*, se conectará al servidor de nombres por default en lugar del servidor local. Esta diferencia es importante conocerla porque es necesario saber si el servidor al que deseamos conectarnos, tal vez no este respondiendo, como se muestra en el siguiente ejemplo:

% nslookup
Default Server: relay.hp.com
Addess: 15.255.152.2

✎ Cuando iniciamos una sesión, nuestro primer servidor, relay.hp.com, se convierte en el lserver.

> server galt.cs.purdue.edu.
Default Server: galt.cs.purdue.edu
Addess: 128.10.2.39

> cs.purdue.edu
Server: galt.cs.purdue.edu
Address: 128.10.2.39

*** galt.cs.purdue.edu, can't find cs.purdue.edu.: No response from server.

✎ En este punto, regresaremos a conectarnos a nuestro servido local original. Pero este servidor de nombres que esta corriendo para *galt*, no podrá encontrar la dirección de *relay*.

> server relay.hp.com.
*** Can't find address for server relay.hp.com.: No response from server.

Para poder hacer esto, nosotros usaremos el comando lserver para regresar al servidor local, y así poder encontrar la dirección de *relay*.

> lserver relay.hp.com.
Default Server: relay.hp.com
Address: 15.255.152.2
>
Desde que el servidor para galt no respondió, aunque ni siquiera estuviera corriendo el servidor, no fue posible encontrar la dirección de relay para conectarse de nueva cuenta al servidor de nombres de relay. Aquí es donde lserver viene al rescate, con el servidor de nombres local de relay. En vez de usar lserver, también se podía regresar usando la dirección IP de relay directamente.

> server 15.255.152.2

Siempre podemos cambiar de servidor desde la base de preguntas. Para especificarle a nslookup que se quiere realizar una búsqueda a un servidor en particular, para obtener información referente a un nombre de dominio, se puede especificar al servidor con un segundo argumento en la línea, después del nombre de dominio que se busca, como en el siguiente ejemplo:

% nslookup
Default Server: relay.hp.com
Address: 15.255.152.2

> pitstop.west.sun.com. sun.com.
Name Server: sun.com
Address: 192.9.9.1

Name: pitstop.west.sun.com
Addresses: 129.153.1.2, 129.145.1.27

>^D

Al cambiarnos de servidor desde la línea de comandos, también se le puede especificar una determinada búsqueda agregándole un argumento después del nombre de dominio que se busca, como se muestra a continuación:

% nslookup -type=mx fisherking.movie.edu. terminator.movie.edu.

Esto le indica a nslookup que busque en terminator.movie.edu el registro mx para el dominio fisherking.movie.edu.
Finalmente, para especificar una alternativa en el servidor de nombres por default, e introducirlo de una manera interactiva, se puede utilizar un guión en lugar del nombre de dominio que se busca.

% nslookup - terminator.movie.edu.

3.1.6 Preguntas menos frecuentes

Estos son algunos trucos que probablemente se tendrán que usar con menos frecuencia, pero que resultan ser muy prácticos, por lo que es necesario tenerlos a la mano. Muchos de éstos, pueden ser muy útiles cuando se está tratando de resolver algún problema en el DNS o en BIND; ellos son capaces de internarse en los paquetes que envía el resolver, e imitar al servidor de nombres de BIND buscando en otro servidor de nombres para llevar a cabo la transferencia de datos de la zona.

Viendo los paquetes de consultas y respuestas.

Si es necesario, podemos hacer que nslookup muestre las consultas que son enviadas, así como las respuestas que son recibidas. Al tener la opción de *debug* en *on*, presentará las respuestas.
A continuación se mostrara un ejemplo de estas consultas, explicándose las partes mas importantes.

```
% nslookup
Default Server: terminator.movie.edu
Address: 0.0.0.0

> set debug
> wormhole
Server: terminator.movie.edu
Address: 0.0.0.0

------------------

Got answer:
HEADER:
        opcode=QUERY, id=6813, rcode=NOERROR
        header flags: response, auth. Answer, want recursion,
        recursion avail. questions=1, answer=2,
        authority records=2, additional=3

 QUESTIONS:
        wormhole.movie.edu, type= A, class=IN
 ANSWERS:
        ☛ wormhole.movie.edu
          internet address=192.253.253.1
          ttl=86400 (1 día)
        ☛ wormhole.movie.edu
          internet address=192.249.249.1
```

ttl=86400 (1 día)
AUTHORITY RECORDS:
- movie.edu
  nameserver=terminator.movie.edu
  ttl=86400 (1 día)
- movie.edu
  nameserver=wormhole.movie.edu
  ttl=86400 (1 día)

ADDITIONAL RECORDS:
- terminator.movie.edu
  internte address= 192.249.249.3
  ttl: 86400 (1 día)
- wormhole.movie.edu
  internet address=192.253.253.1
  ttl: 86400 (1 día)
- wormhole.movie.edu
  internet address=192.249.249.1
  ttl: 86400 (1 día)

Name: wormhole .movie.edu
Addresses: 192.253.253.1, 192.249.249.1

> set d2
> wormhole
Server: terminator.movie.edu
Address: 0.0.0.0

En este momento solo se muestra la consulta

SendRequest(), len 36
HEADER:
opcode=QUERY, id=6814, rcode=NOERROR
header flags: query, want recursion
questions=1, answers=0, authority records=0,
additional=0

QUESTIONS:
wormhole.movie.edu, type=A, class=IN

- - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - -

Got answer (164 bytes):

Esta respuesta es la misma que la de arriba.

El texto que se muestra entre los guiones, son los paquetes de consulta y de respuesta. Ahora se tratara de explicar cada una de las partes.
Los paquetes del DNS se componen de 5 secciones:
1.- Sección de cabecera (Header section)
2.- Sección de consulta (Question section)
3.- Sección de respuesta (Answer section)
4.- Sección de autoridad (Authority section)
5.- Sección adicional (Additional section)

☑ Sección de cabecera (Header section)

La sección de cabecera se presenta en cada consulta y cada respuesta. El código de operación es siempre QUERY. Algunos otros tipo de código (opcodes) son IQUERY y STATUS, pero éstos no son utilizados. El id es usado para asociar la respuesta con la consulta y detectar consultas o respuestas duplicadas. Se tiene que observar el apuntador de la cabecera para verificar cuales son paquetes de consultas y cuales de respuestas. La cadena *want recursion* significa que la consulta quiere que el servidor de nombres haga todo el trabajo. El apuntador se repite en la respuesta. La cadena *auth. answer* significa que la respuesta es autoritaria. En otras palabras, quiere decir que los datos de la respuesta vienen desde el servidor de nombres que es autoridad, y no de los datos del cache. El código de respuesta, rcode, puede tener las siguientes opciones: no error, server failure, name error, not implemented o refused. Los códigos de respuesta server failure, name error, not implemented y refused ocasionan en el nslookup, que el servidor falle, que no exista el dominio, que no se implemente y que rechace la consulta, respectivamente.
Las siguientes cuatro entradas en la cabecera, son contadores que indican cuantos *resource records* hay en cada una de las siguientes cuatro secciones.

☑ Sección de consulta (Question section)

Esta es siempre una consulta en el paquete del DNS; éste incluye el nombre, el tipo y la clase de datos de la respuesta.
La capacidad de manipulación, más que una consulta en el paquete del DNS, podría requerir un rediseño en el formato de los paquetes. Por una parte, el simple bit de autoridad, podría cambiarse,

porque la sección de respuestas podría contener una mezcla de respuesta autoritarias y no autoritarias. En el presente diseño, el bit de respuesta autoritaria, significa que el servidor de nombres es autoridad para el nombre de dominio en la sección de consulta.

☑ Sección de respuesta (Answer section)

Esta sección contiene los *resource records* de la respuesta. Puede haber más de un resource records en la respuesta. Por ejemplo, si el host es *multihomed* podría haber más de un resource record Address (A).

☑ Sección de autoridad (Authority section)

La sección de autoridad, es a donde se dirige el registro del servidor de nombres. Cuando una respuesta se refiere a una consulta hacia otro servidor de nombres, éste servidor de nombres se lista aquí.

☑ Sección adicional (Additional section)

En la sección del registro adicional, se agregan los datos que pueden completar la información incluida en otras secciones. Por ejemplo, si un servidor de nombres se enlista en la sección de autoridad, la dirección del servidor de nombres se agrega en la sección del registro adicional. Después de todo, para poder contactar a un servidor de nombres, se necesita tener la dirección IP del servidor.

Cómo realizar las búsquedas tal y como un servidor de nombres?

Se puede hacer que nslookup envíe un paquete de consultas tal y como el servidor de nombres lo hace. Los paquetes de consulta de un servidor de nombres no son muy diferentes a los paquetes del resolver. La principal diferencia en los paquetes es que el resolver pide servicios recursivos, y el servidor de nombres raramente lo hace.
La recursión es por default en el nslookup, pero se tiene la posibilidad de anular esa opción. La diferencia en la operación entre el resolver y el servidor de nombres, es que el resolver implementa una lista de búsqueda, y el servidor de nombres no lo hace. Por default, nslookup implementa una lista de búsqueda, pero también se pude anular esta opción.
En realidad el término nslookup significa hacer las consultas como un resolver, usando los valores por default. Para realizar búsquedas tal y como lo hace el servidor de nombres, se debe usar *set norecurse* y *set nosearch*. En la línea de comando se colocaría de la siguiente manera:

nslookup -norecurse -nosearch

Cuando el servidor de nombres realiza una consulta, éste ve si tiene la respuesta en caché. Si no encuentra la respuesta, y si es autoridad para el dominio, el servidor de nombres contesta que el

nombre no existe o que no existen datos para ese tipo. Si el servidor de nombres no tiene la respuesta, y no es autoridad para el dominio, éste empieza a recorrer el árbol de los dominios buscando los registros NS. Pueden ser los registros NS de cualquiera de los niveles del árbol o bien los registros NS de los dominios de la raíz del nivel más alto.
Si el servidor de nombres recibe una búsqueda no recursiva, este podría responder con una consulta dando los registros NS que haya encontrado. Por otro lado, si la consulta original fue una consulta recursiva, el servidor de nombres consultaría a un servidor de nombres remoto en los registros NS hasta encontrar la respuesta. Cuando el servidor de nombres recibe respuesta desde un servidor de nombres remoto, el cache responde, y repite el proceso si es necesario. El servidor de nombres remoto, contestaría dando la respuesta a la consulta solicitada, o tendría la lista de los servidores de nombres de un nivel mas abajo del árbol para finalizar con la pregunta.
Como ejemplo, se puede asumir que se está tratando de llevar a cabo una consulta recursiva pero que no se encuentra ningún registro NS mientras se esta verificando el dominio *com*. Este es un caso en donde se preguntará al servidor de nombres en relay.hp.com sobre el dominio skyler.mavd.boneywell.com, por lo que no encontrará ningún registro NS mientras se encuentre en el dominio com. Aquí es en donde contactaremos al servidor con un servidor de nombres para el dominio com y se le hará la misma pregunta. Enseguida nos enviará al servidor para el dominio honeywell.com, nos conectaremos a este servidor y realizaremos la misma pregunta.

```
% nslookup
Default Server: relay.hp.com
Address: 15.255.152.2
> set norec                    - Se hará una consulta como un servidor de
                                 nombres. Se coloca en off la recursión.
> set nosearch                 - Se cambiará a off la opción de búsqueda de
                                 listas.
> skyler.mavd.honeywell.com    - Aquí no se necesita un punta al final puesto
                                 se cambió a search off.

Server: relay.hp.com
Address: 15.255.152.2

Name: skyler.mavd.honeywell.com
Served by:
- H.ROOT-SERVERS.NET
128.63.2.53
 com
- B.ROOT-SERVERS.NET
 128.9.0.107
 com
- C.ROOT-SERVERS.NET
 192.33.4.12
 com
```

- D.ROOT-SERVERS.NET
128.8.10.90, 128.8.10.7
com
- E.ROOT-SERVERS.NET
192.203.230.10
com
- I.ROOT-SERVERS.NET
192.36.148.17, 192.36.148.214
com
- F.ROOT-SERVERS.NET
39.13.229.241, 192.5.5.241
com
- G.ROOT-SERVERS.NET
192.112.36.4, 192.192.4.56
com
- A.ROOT-SERVERS.NET
198.41.0.4
com

✎ Conectarse al servidor de nombres para el dominio com. Se debe poner temporalmente la opción de recursión, en caso de que el servidor de nombres no tenga la dirección lista en caché.

> server e.root.servers.net
Default Servers: e.root-servers.net
Address: 192.203.230.10

✎ Preguntarle lo mismo al servidor de nombres para com.

> skyler.mavd.honeywell.com
Server: e.root-servers.net
Address: 192.203.230.10

Name: skyler.mavd.honeywell.com
Serverd by:
- FISHERY.HONEYWELL.COM
129.30.3.16
HONEYWELL.COM
- SRC.HONEYWELL.COM
129.235.16.19
HONEYWELL.COM

- NS.MR.NET
137.192.240.5
HONEYWELL.COM

✐ Conectarse al servidor de nombres para el dominio honeywell.com, con cualquiera de las tres opciones.

> server src.honeywell.com
Default Server: src.honeywell.com
Address: 129.235.16.19

✐ Se hace la misma pregunta al servidor de nombres para el dominio honeywell.com. Éste servidor nos puede dar referencia del servidor de nombres para el dominio mavd.honeywell.com, o nos puede contestar la pregunta si este es el servidor de nombres para ese dominio.

> skyler.mavd.honeywell.com
Server: src.honeywell.com
Address: 129.235.16.19

Name: skyler.mavd.honeywell.com
Address: 146.167.60.60

Con este ejemplo, se puede apreciar que a todos los servidores se les hizo la misma pregunta. ¿Cuál es la dirección de skyler.mavd.honeywell.com? ¿Que piensas que hubiera pasado si el servidor de nombres de com hubiera tenido en caché la dirección de skyler?
El servidor de nombres para el dominio com, podía haber tenido la respuesta en caché en vez de habernos dado la referencia del servidor de nombres para honeywell.com. Este asunto es significante porque supongámonos que en algún momento llegamos a tener un desorden en las direcciones de los host de nuestro dominio. Alguien nos indica que lo arreglemos, y así lo hacemos. Aunque nuestro servidor de nombres tenga ahora los datos correctos, en algún lugar remoto, pueden encontrarse los datos incorrectos, debido a que en un pasado se hizo la búsqueda de un nombre. Uno de los servidores de nombres de un nivel mas alto del árbol de dominios, busca en los servidores de nombres de la raíz, que tienen en cache los datos incorrectos. Cuando éstos reciben la consulta por la dirección del host, éstos le regresan datos incorrectos, en vez de hacer referencia a nuestro servidor de nombres.
Lo que hace a este problema difícil de resolverse desde abajo, es que solo uno de los servidores de nombres de mas arriba tiene en cache los datos incorrectos, y solo uno de los remotos buscadores obtuvo la respuesta incorrecta, el único que uso este servidor.
Una de las soluciones a este problema es esperar a que en el servidor de nombres que tiene datos incorrectos en cache se termine el tiempo que se establece para tener guardados los datos en cache, o bien contactar al administrador de ese servidor para que inicialice nuevamente el *named* y así eliminar todo lo que guardaba en caché.

Transferencia de zonas.

Nslookup puede usarse para realizar transferencia total de zonas con el comando *ls*. Esta característica es usada para resolver problemas, para deducir como deletrear un nombre de un host remoto, o para contar cuantos host hay en algún dominio remoto. Los datos resultantes de la ejecución de éste comando pueden se dirigidos a un archivo y verlos después con el comando *more*. Si queremos salirnos a mitad de la transferencia, se puede hacer tecleando cualquier carácter de interrupción de procesos.

Cuidado: algunos host no dejan hacer copias de los datos de su zona, ya sea por razones de seguridad o por no dejar cargado de datos al servidor de nombres. Internet es un lugar amistoso, pero los administradores tienen que defender su territorio. Hay que recordar que un servidor de nombres puede engendrar varios procesos hijos y manejar la transferencia de zonas. Si el servidor de nombres es un proceso muy grande, tal vez el administrador no desee que se produzcan muchos procesos hijos, ya que el servidor podría caerse.

Este no es un mecanismo que limite cuantos procesos hijos pueden inicializarse en el servidor de nombres como respuesta a las peticiones de datos de una zona, es el administrador el que se encarga de poner un limite de cuantos hosts pueden realizar una copia de los datos de la zona.

Como ya se había mencionado, nslookup filtra los datos de una zona. Solo muestra algunos datos de ésta a menos que se le indique que lo haga de otra manera. Por omisión, solo se pueden ver las direcciones y los datos de los servidores de nombres. Se podrían ver todos los datos de la zona si se le indica a nslookup que muestre los datos de cualquier tipo. Con la información de las zonas, se pueden producir muchos tipos de salidas, y ridireccionarlos a un archivo. En este trabajo, solo se mostrara a grandes rasgos el funcionamiento del parámetro -t para el comando ls. El parámetro -t toma un argumento: un tipo de dato para ser filtrado. Para realizar una copia de la zona y ver todos los datos del registro mx, se teclearía el comando de la siguiente manera.

ls -t mx domain

```
% nslookup
Default Server: terminator.movie.edu
Address: 0.0.0.0

> ls movie.edu.                    - Se enlistan los registros NS y A para movie.edu
[terminator.movie.edu]
movie.edu.              server = terminator.movie.edu
terminator              192.249.249.3
movie.edu               server = wormhole.movie.edu
wormhole                192.249.249.1
wormhole                192.253.253.1
robocop                 192.249.249.2
shining                 192.253.253.3
localhost               127.0.0.1
```

```
carrie                  192.253.253.4
diehard                 192.249.249.4
misery                  192.253.253.2

> ls -t mx movie.edu.   - Lista los registros mx
[terminator.movie.edu]
wormhole        10      wormhole.movie.edu
robocop         10      robocop.movie.edu
shining         10      shining.movie.edu
terminator      10      terminator.movie.edu
carrie          10      carrie.movie.edu
diehard         10      diehard.movie.edu
misery          10      misery.movie.edu

> ls -t any movie.edu > /tmp/movie      - lista todos los datos y los coloca en
                                          /tmp/movie.
[terminator.movie.edu]
Received 19 records.

> view /tmp/movie                       - ve los datos en el archivo
carrie                  A       192.253.253.4
carrie                  MX      10      carrie.movie.edu
diehard                 A       192.249.249.4
diehard                 MX      10      diehard.movie.edu
localhost               A       127.0.0.1
misery                  A       192.253.253.2
misery                  MX      10      misery.movie.edu
movie.edu.              NS      terminator.movie.edu
movie.edu.              NS      wormhole.movie.edu
movie.edu.              SOA     terminator.movie.edu
(root.terminator.movie.edu.     1       10800 3600    604800     86400)
movie.edu.              SOA     terminator.movie.edu
(root.terminator.movie.edu.     1       10800 3600    604800     86400)
robocop                 A       192.249.249.2
robocop                 MX      10      robocop.movie.edu
shining                 A       192.253.253.3
shining                 MX      10      shining.movie.edu
terminator              A       192.249.249.3
terminator              MX      10      terminator.movie.edu
wormhole                A       192.249.249.1
wormhole                A       192.253.253.1
wormhole                MX      10      wormhole.movie.edu
```

Además del parámetro -t existen otros como son:

-a Lista los aliases de los hosts en el dominio. Es similar a teclear -t CNAME.
-d Lista todos los registros del dominio . Similar a teclear -t ANY.
-h Lista el CPU y la información de los sistemas operativos del dominio. Similar a teclear -t HINFO.
-s Lista los servicios conocidos del host en el dominio.

3.1.7 Resolviendo los problemas de nslookup

Lo último que se quisiera, es tener problemas con la herramienta de solución de problemas. Algunos tipos de fracasos en el rendimiento de la herramienta, son algo tontos. Otros tipos de fracasos en nslookup, son en el mejor de los casos, confusiones porque no se brinda ninguna información directa de como trabajar con él. Pueden ser realmente pocos los problemas que se presentes con nslookup, pero muchos de éstos se pueden deber a configuración u operación de los servidores. Algunos de los problemas más comunes con los que nos podemos encontrar son los siguientes.

Buscando datos correctos

Éste no es realmente un problema, pero puede presentar una gran confusión. Si se usa nslookup para buscar algún tipo de dato de un nombre de dominio, y el nombre de dominio existe, pero no los datos que se están buscando, se puede tener un error como el siguiente:

```
% nslookup
Default Server: terminator.movie.edu
Address: 0.0.0.0

> movie.edu.
*** No address (A) records available for movie.edu.
```

Este mensaje indica que el registro A no existe para el dominio movie.edu, pero ¿como que no existe?
Para esto es necesario escribir:

```
> set type = any
> movie.edu.

Server: terminator.movie.edu
Address: 0.0.0.0

movie.edu
        origin = terminator.movie.edu
```

mail addr = al.robocop.movie.edu
serial =42
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
minimum = 86400 (1 day)

movie.edu nameserver = terminator.movie.edu
movie.edu nameserver = wormhole.movie.edu
movie.edu nameserver = zardoz.movie.edu
movie.edu preference = 10, mail exchanger = postmanrings2x.movie.edu
postmanrings2x.movie.edu internet address = 192.249.249.66

No hay respuesta desde el servidor

¿ Que pudo haber pasado si el servidor no encuentra su propio nombre?

% nslookup
Default Server: terminator.movie.edu
Address: 0.0.0.0

> terminator
Server: terminator.movie.edu
Address: 0.0.0.0

*** terminator.movie.edu can't find terminator: No response from server

El mensaje de error "no response from server" significa que el servidor de nombres no nos puede regresar una respuesta. Nslookup no necesariamente busca cualquier cosa cuando inicia. Si vemos que la dirección del servidor es 0.0.0.0, nslookup grabará el nombre del host del sistema (que el comando hostname regresa) para el campo del servidor y regresará al prompt. Si esto se presenta únicamente cuando se trata de buscar algo que se encontró fuera del servidor que no está respondiendo. En este caso, es obvio que no es un servidor que no este corriendo, sino que es un servidor de nombres que no es capaz de buscar su propio nombre. Si se esta buscando alguna información remota, aunque el servidor de nombres pueda fracasar en dar una respuesta porque todavía continua tratando de buscar y nslookup abandona la espera. Por lo tanto, ¿como se puede distinguir la diferencia entre si un servidor no esta corriendo o el servidor está corriendo pero no responde? Se usará el comando ls para distinguir estas diferencias:

% nslookup
Default Server: terminator.movie.edu
Address: 0.0.0.0

> ls foo. - Trata de listar un dominio no existente
*** Can't list domain foo.: No response from server

En este caso, el servidor no esta corriendo. Si el host no puede ser alcanzado, el error podría ser "tiempo fuera -time out-" . Si el servidor de nombres está corriendo, se podría ver el siguiente mensaje de error:

% nslookup
Default Server: terminator.movie.edu
Address: 0.0.0.0

> ls foo.
[terminator.movie.edu]
*** Can't list domain foo.: No information

Esto seria válido a menos que foo fuera un dominio del top- level en nuestro mundo (Que no lo es).

No existen datos PTR para la dirección del servidor de nombres

Este es uno de los problemas mas molestos: algo se dañó y nslookup se salió al inicilizarse.

% nslookup
*** Can't find server name for address 192.249.249.3: Non-existent host/domain
*** Default servers are not available

El mensaje "Non-existent domain" significa que el nombre 3.249.249.192.in-addr.arpa no existe. En otras palabras, nslookup no puede encontrar el nombre para 192.249.249.3, que es el host del servidor de nombres. Si se crea el archivo resolv.conf que incluye las líneas con los nombres de los servidores, nslookup busca las direcciones en el orden que obtiene los nombres de los servidores. En el ejemplo, éste es un servidor de nombres que está corriendo en 192.249.249.3, pero indica que no hay datos PTR para la dirección 192.249.249.3. Obviamente, este servidor de nombres tiene desordenados los datos, o por lo menos para el dominio 249.249.192.in-addr.arpa.
El mensaje de "Default servers are not available" no se le toma importancia, ya que en este caso el problema real es que no encuentra la dirección. Con más frecuencia, se puede ver el mensaje de error "no response from server", que indica que el servidor de nombres no está corriendo en el host o el host está siendo rechazado. En este caso, es cuando el mensaje de "default servers are not available" tiene sentido.

Consulta rechazada

El rechazo de las consultas pueden ser causados por problemas en la inicialización, y ellos pueden causar búsquedas fallidas durante las sesiones. Aquí se verá un ejemplo de cuando nslookup se sale en la inicialización rechazándose la consulta.

```
% nslookup
*** Can't find sever name for address 192.249.249.3: Query  refused
*** Default servers are not available
%
```

Esta problema puede ser originado por dos posibles causas; o el servidor de nombres no soporta consultas inversas (sólo en versiones anteriores de nslookup), o porque la seguridad de la zona detiene la consulta.
Las versiones antiguas de nslookup (antes de la 4.8.3) usan una consulta inversa al inicializar. Las consultas inversas nunca se utilizaron ampliamente - nslookup fue una de las pocas aplicaciones que no las usaron. Hasta antes de la versión 4.9.3, el soporte de las consultas inversas fué bajo. Para acomodar estos clientes viejos, en el archivo de inicialización se agregó la directiva: options fake-iquery. Esta directiva permitía que el servidor de nombres respondiera a las consultas inversas con una respuesta "falsa" que era lo suficientemente bueno para que nslookup continuara trabajando.
La reciente adición a la característica de seguridad de las zonas, ocasionó que nslookup iniciara con problemas. Cuando nslookup intentaba encontrar un nombre en el servidor (usando búsquedas de PTR y no con consultas inversas) las consultas eran rechazadas. Si se piensa que el problema es la seguridad de la zona, se debe estar seguro que los registros TXT de la zona de seguridad, incluye la red en la que se encuentra el host en el que está corriendo nslookup, y la dirección 127.0.0.1 si nslookup está corriendo en el host en el que también está corriendo el servidor de nombres.
La seguridad de las zonas, no ocasionan que nslookup fracase en la inicialización. Esto solo puede causar que las búsquedas y las transferencias de zonas fallen a mitad de la sesión cuando nslookup se apunta a un servidor de nombres remoto.
Algo que se podría llegar a ver sería lo siguiente:

```
% nslookup
Default Server: hp.com
Address: 15.255.152.4
> server terminator.movie.edu
Default Server: terminator.movie.edu
Address: 192.249.249.3

> carrie.movie.edu.
Server: terminator.movie.edu
Address: 192.249.249.3
*** terminator.movie.edu can't find carrie.movie.edu.: Query refused
```

> ls movie.edu - Con esto se intenta la transferencia de zona
[terminator.movie.edu]
*** Can't list domain movie.edu: Query refused
>

El primer servidor de nombres del resolv.conf no responde

Este es otro de los errores comunes que suelen aparecer:

% nslookup
***Can't find server name address 192.249.249.3: No response from server
Dafault server: wormhole.movie.edu
Address: 192.249.249.3

En este momento el primer servidor de nombres que se encuentra declarado en el resolv.conf no está respondiendo. Para esto, se tiene que colocar un segundo servidor de nombres en el resolv.conf , y así el segundo servidor responderá. De ahora en adelante, nslookup enviará las consultas solo a wormhole, y ya no querrá enviarlas al servidor de nombres 192.249.249.3 nuevamente.

3.2 DIG

Dig (Domain Information Grouper) es otra de las herramientas con las que el DNS envía consultas otros servidores e imprime las respuestas. Muchos piensan, en su mayoría ingenieros en redes, que ésta herramienta es más útil que nslookup. El WEB, permite usar código en Perl para hacer consultas vía Dig. Éste software también está disponible como una parte más de BIND.
Las salidas que proporciona Dig, comienzan con información referente a los comandos emitidos y el o los servidores de nombres utilizados, los apuntadores usados en el resolver y los mensajes del DNS decodificados como respuesta. Después presenta el campo de cabecera y sus apuntadores, seguido por la respuesta, registro de autoridad, y una sección de registro adicional. Cada una de éstas secciones contiene cero o más resource records, los cuales se presentan con un formato adecuado para ser entendibles; empezando con el nombre del dominio, el tiempo de vida (Time-to-live), el tipo de código y por último el campo de datos. Finalmente, se presenta información adicional de la transferencia de los datos.
A continuación se presenta la impresión de una salida de Dig:

tower:~$dig@ns.adnc.com FreeSoft.org mx

[1] ; <<>> Dig 2.1 <<>> @ns.adnc.com FreeSoft.org mx
[2] ; (1 server found)
[3] ;; res options: init recurs defnam dnsrch
[4] ;; got answer:
[5] ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10

```
[6]   ;; flags: qr aa rd ra; Ques: 1, Ans: 1, Auth: 2, Addit: 2
[7]   ;; QUESTIONS
[8]   ;;      FreeSoft.org, type = MX, class = IN
[9]
[10]  ; ANSWERS:
[11]  ; FreeSoft.org.      86400      MX    100 mail.adnc.com.
[12]
[13]  ;: AUTHORITY RECORDS:
[14]  ; FreeSoft.org.      86400      NS    ns.adnc.com.
[15]  ; FreeSoft.org.      86400      NS    ns2.adnc.com.
[16]
[17]  ;; ADDITIONAL RECORDS:
[18]  ns.adnc.com.         86400      A     205.216.138.22
[19]  ns2.adnc.com.        86400      A     205.216.138.24
[20]
[21]  ;; Total query time: 464 msec
[22]  ;; FROM: tower to SERVER: ns.adnc.com  205.216.138.22
[23]  ;; WHEN: Tue Mar 19  20:31:58  1996
[24]  ;; MSG SIZE sent: 30  rcvd: 126
```

El argumento principal en la petición de Dig, es FreeSoft.org, el nombre del dominio en donde se realizará la consulta. El primer argumento, @ns.adnc.com es opcional y especifica el nombre del servidor que se usará (normalmente el sistema por default lo escoge). El siguiente argumento especifica el *querytype*, en este caso se hará para el registro mail exchanger (MX). Este argumento es opcional, ya que el registro por default es address (A).

Continuando línea por línea (se enumero solo por conveniencia), generalmente no aparece la numeración de líneas. Las primeras dos líneas repiten los argumentos que anteriormente se dieron para iniciar la consulta. Si Dig se retarda después de haber presentado las primeras líneas, tal vez exista una falla en la configuración del servidor de nombres; trata de reemplazar el nombre ns.adnc.com con su respectiva dirección IP.

A continuación, se verá las opciones del resolver, las cuales están documentadas en el manual del resover de BIND.

En la línea 5 se pueden ver varias opciones de la cabecera del *reply*.

Seguimos con varios de los resouce records. En la línea 11 aparece el nombre del dominio y el tipo de información por los que preguntamos. El registro autoridad (línea 14-15) nos informa que el servidor de nombres (ns.adnc.com) es autoridad para este registro, así como ns2.adnc.com. Sin sorprendernos, podemos notar que se colocó el bit aa como bandera (línea 6), por lo que en el registro adicional (línea 18-19) se presentan las direcciones IP de los servidores de nombres.

Finalmente, se puede ver (línea 21) el tiempo de transferencia, indicaciones del remoto servidor de nombres y su dirección IP (línea 22), la fecha en la que se hizo la transferencia (línea 23), así como el tamaño de la consulta y la respuesta (línea 24).

De esta manera se pueden hacer un gran número de consultas, pero la presentación de los datos siempre será la misma.

CAPITULO 4 "EL SISTEMA DE NOMBRES DE DOMINIO (DNS) EN REDUNAM"

Después de haber estudiado las características y el funcionamiento del sistema de nombres de dominio, ahora se realizará un estudio de los servidores de nombres de la UNAM, en los cuales se lleva a cabo el manejo del DNS y de los dominios tanto de dependencias de la UNAM, como también de instituciones externas, siendo NICunam el responsable de la administración.

4.1 ESTRUCTURA DE REDUNAM

Para las universidades mexicanas Internet representa una poderosa herramienta para acercar a los estudiantes a un cúmulo de información reciente, estimulando su interés hacia la investigación y la comunicación con jóvenes universitarios e instituciones de alto nivel, buscando concretar una formación educativa integral.

RedUNAM es el proyecto desarrollado para la transmisión de datos entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias que conforman a la UNAM.

El final de los años 60's y el principio de la década de los 70's marcaron para la UNAM, la etapa de inicio de las comunicaciones telefónicas y de datos. Es en este periodo cuando se realizan las primeras conexiones de teletipos hacia una computadora central, utilizando líneas telefónicas de cobre, de la recién instalada red telefónica dentro de la institución.

Rápidamente esta tecnología es usada al interior de la UNAM y difundida al exterior, por ello se efectúan una gran cantidad y diversidad de conexiones, de terminales de caracteres, de graficación e impresión, hasta la interconexión de estaciones de trabajo manejando líneas telefónicas. A partir de la segunda parte de la década de los 80's surge en la UNAM la búsqueda de cambios en las comunicaciones.

Así en 1987, la UNAM establece la primera conexión a la Red Académica de C o BITNET, mediante enlaces telefónicos, desde la Ciudad Universitaria hasta el Instituto Tecnológico de Estudios Superiores de Monterrey y de ahí hasta San Antonio, Texas en los E.U.A.

No fue sino hasta 1989, cuando la UNAM a través del Instituto de Astronomía establece un convenio de enlace a la red de la NSF en E.U.A, el cual se realizó utilizando el satélite mexicano Morelos II entre el Instituto de Astronomía en la UNAM y el UCAR-NCAR con residencia en Boulder Colorado, además, se llevó a cabo el primer enlace para conectar las redes de área local, entre el Instituto de Astronomía y la Dirección General de Servicios de Cómputo Académico, utilizando enlaces de fibra óptica.

A partir de ese momento se inició dentro de la UNAM una revolución en las comunicaciones, así como la adquisición masiva de computadoras personales y su intercomunicación en redes de área local, principalmente en las dependencias del subsistema de la investigación científica; lo cual permitió desarrollar la infraestructura de comunicaciones con fibra óptica, y establecer más enlaces satelitales hacia Cuernavaca, Mor. y San Pedro Mártir en Ensenada Baja California Norte, a la par del primer enlace de microondas de alta velocidad entre la Torre II de Humanidades y la Dirección General de Servicios de Cómputo Académico, DGSCA, sobre la Ciudad de México.

Con esto último, se estableció en definitiva el final de la era del teleproceso, para dar paso a las redes de computadoras y sus enlaces a través de fibra óptica. En 1990 la UNAM, fué la primera institución en Latinoamérica que se incorpora a la red mundial Internet, que enlaza a millones de máquinas y decenas de millones de usuarios en todo el mundo.

4.2 NICUNAM

Como actividad inicial, el NIC se encarga del mantenimiento de una Base de Datos donde se concentra la información concerniente a la administración de las Redes e Instituciones.
REDUNAM está compuesta por un conjunto de redes locales que tiene una administración propia, pero al estar conectadas a toda la red sus encargados y usuarios deben acatar las disposiciones establecidas por la Dirección de Telecomunicaciones con representación por parte del NICunam; lo que representa un esquema de administración jerárquica.
Los servicios que ofrece el NICunam están orientados básicamente a las necesidades generales de cada una de las redes locales como son:

Servicio de Nombres.

Actualmente todos los hosts cuentan con una dirección IP y un nombre, el cual está asociado al dominio UNAM.MX. Esto les permite ser identificados dentro de Internet y poder tener comunicación con otros hosts, sobre todo en aplicaciones como el correo electrónico. Por ello es conveniente que cada uno de ellos esta dado de alta en las Bases de Datos del Servicio de Nombres; esto se hace mediante una solicitud que envía el administrados de la red local al NICunam.

Asignación de Direcciones IP

El esquema de direccionamiento que se utiliza en REDUNAM está basado en Direcciones IP. El NIC asigna a cada una de las dependencias que se conectan a la red un segmento o un rango de direcciones IP; el administrador de la red local es el responsable de hacer esta solicitud al NIC. Una vez hecha la asignación, esta persona es la encargada de asignar una direción IP a cada uno de los hosts que conforman a la red de la dependencia. De la misma forma se asignan clases de direcciones IP a instituciones independientes a la UNAM que se conectan a la red universitaria, y que así lo requieren. El NIC se reserva el derecho de ceder o retirar la administración total o parcial de las subredes a quien considere conveniente de acuerdo a las normas de uso aceptable de REDUNAM y buscando siempre el mejor desempeño de la administración de la misma red.

Asignación y Solicitud de Dominios

En el caso de dependencias de la UNAM, el NIC le asigna a cada una de ellas un subdominio bajo UNAM.MX, previa solicitud del administrador local. Para las instituciones externas, el NIC de la UNAM hace la solicitud de dominios ante NIC-México para aquellas que así lo requieran.

nicunam

Centro de Información de RedUNAM

UNAM

El Centro de Información de RedUNAM (NICunam) tiene como objetivo primordial proveer información técnica y administrativa acerca de la **Red de Datos de la UNAM** e Internet; así como el establecimiento de políticas que permitan su eficiente administración.

- INFO. NICUNAM
- BUSQUEDA
- NOTICIAS
- FAQ-NICUNAM
- INTERNET
- PERSONAL
- LOGIN

última actualización: 06 OCTUBRE 1998 Tel. 622 8110

Servicio de Servidor Secundario.

En muchas ocasiones, instituciones ajenas a la Universidad requieren de tener un servidor secundario para sus dominios; el NIC ofrece este servicio a aquellas que están directamente conectadas a REDUNAM.

Elaboración e Implementación de Políticas

Este es uno de los pilares para la administración de REDUNAM. El NIC elabora políticas concernientes a cada uno de los servicios que brinda y de acuerdo a las necesidades de administración. Este trabajo se lleva a cabo en conjunto con los diversos grupos de trabajo que intervienen en la operación de la red universitaria.
Por medio de los diferentes servicios de información da a conocer a los administradores de red y a la comunidad universitaria los lineamientos que se deben seguir para hacer uso de servicios, petición de direcciones IP, solicitud de dominios, etc. Los administradores de red deben estar de acuerdo con estas políticas y es su responsabilidad hacerlas del conocimiento de sus usuarios.

4.3 Políticas de Asignación de Dominios y Direcciones IP

4.3.1 Políticas de Asignación de dominios

Se entiende por "Asignar" al hecho de autorizar a los responsables de una dependencia la utilización de un dominio con el objetivo de asociarlo a sus direcciones IP, así como la posibilidad de enviar solicitudes de altas y/o bajas de nombres, alias y/o mail exchangers relacionados al mismo.
Cualquier solicitud o trámite de asignación debe ser realizado mediante los formatos y procedimientos establecidos por NICunam, que es el encargado de la administración de este recurso de Internet para REDUNAM.

Dominios bajo UNAM.MX

Este tipo de dominios solo pueden ser asignados a las Dependencias a las que ya se les haya asignado un rango de direcciones IP con anterioridad.
El nombre del dominio debe cumplir con las siguientes normas:

- Su longitud puede ser de 14 caracteres como máximo.
- Los caracteres permitidos son letras, números y/o guiones.
- Un nombre de dominio no puede empezar ni terminar con guión.
- No se aceptan guiones bajos (_).
- Se recomienda que el nombre de dominio haga referencia al nombre de la dependencia o sus iniciales.

La solicitud de asignación de dominio deberá hacerse por medio del formato de Web o, en su defecto, a través de correo electrónico.

a) Soliciud a través de Web:
   - ✓ Ingresar el URL *http://www.nic.unam.mx*
   - ✓ Ingresar a la liga: *Formas de registro*
   - ✓ Ingresar a la liga: *Asignación de dominios*
   - ✓ Llenar los campos de la forma de registro con los datos correctos

b) Solicitud a través de Correo Electrónico:
   - ✓ Bajar el formato de texto vía ftp y seguir las instrucciones indicadas al final del archivo:

   ftp://ftp.nic.unam.mx/Formas/Dominio-Solicitud

La información contenida en la solicitud será verificada y ratificada de acuerdo a la Base de Datos de NICunam. En este caso de encontrarse información falsa o no congruente, la solicitud será rechazada y se notificará a los responsables de la dependencia y al solicitante.
Las solicitudes serán procesadas de acuerdo al orden en que se reciban.
Solo podrán ser procesadas aquellas solicitudes que provengan de:

- ✓El responsable administrativo (E-mail asociado)
- ✓El responsable técnico (E-mail asociado)

Los tipos de movimientos que se pueden realizar sobre los dominios son:

- ALTA. La dependencia debe tener al menos un rango de direcciones IP y toda la información de responsables, en orden.
- BAJA. Sólo podrá ser realizada cuando exista el dominio y provenga de alguno de los responsables.
- ACTUALIZACIÓN. El objetivo de hacer una actualización de dominio es con el fin de modificar la información relacionada a éste, no el dominio.
- CAMBIO DE NOMBRE DE DOMINIO. Este movimiento procederá siempre y cuando haya concensado a nivel de los usuarios del dominio. La información relacionada a los responsables y la institución deberá permanecer igual.

Para este proceso, NICunam mantiene activo el dominio viejo por un periodo de 60 días y lo elimina una vez concluído el lapso. El dominio nuevo queda trabajando junto con el viejo; esto es con el fin de evitar problemas de recepción de correo electrónico y dar tiempo a la publicidad de nuevo dominio. Después de 60 días, NICunam no se hace responsable por problemas relacionados con el dominio viejo debido a falta de publicidad y planeación por parte de los responsables.

Los servidores de nombres para los dominios solicitados por las dependencias y usuarios, serán los servidores de nombres oficiales para dominios de la UNAM:

dns1.unam.mx	132.248.204.1
dns2.unam.mx	132.248.10.2
dns3.unam.mx	132.248.64.250
dns4.unam.mx	132.248.237.250

Tanto el responsable administrativo como técnico deberán conocer y respetar estas políticas, haciéndolas del conocimiento de todos sus usuarios.

Dominios Independientes de UNAM.MX

Se entiende por dominio independiente de UNAM.MX, a todo aquel dominio que se desee asociar a un host o conjunto de hosts de una dependencia de la UNAM con el fin de albergar servicios de Internet (principalmente WWW y correo electrónico) ajenos a la UNAM.
Para la asignación de este tipo de dominios aplican los puntos mencionados en Dominios bajo UNAM.MX y se complementan con los siguientes.

A) Asignación para dependencias de la UNAM

- Se debe enviar una justificación detallada y concreta de la razón de asociar un dominio de este tipo a hosts de la UNAM.
- Para que la solicitud pueda proceder, los hosts a los cuales se asociaría el dominio deben de pertenecer a un dominio bajo UNAM.MX previamente.
- Por norma, el organismo facultado para autorizar y administrar los servidores de nombres para este tipo de dominios es NICunam.
- La solicitud de dominios de tipo comercial (com, net), o de asociación civil (org) son sujetos a aprobación, independientemente de su justificación.
- En este tipo de dominios se aplican la políticas de NIC-México e InterNIC en cuanto a longitud máxima y caracteres permitidos.
- Cumplir con el formato de solicitud

B) Asignación a usuarios con servicio de alojamiento de equipo de cómputo

- De acuerdo a los convenios y contratos para este tipo de servicio, el dominio deberá ser solicitado a NICunam debido a que la dirección IP que se asigna al equipo pertenece a la UNAM.
- En este tipo de dominios se aplican la políticas de NIC-México e InterNIC en cuanto a longitud máxima y caracteres permitidos.
- Cumplir con el formato de solicitud

Centro de Información de RedUNAM

Solicitud de Dominios

TIPO DE SOLICITUD

- (●) ALTA
- ( ) BAJA
- ( ) ACTUALIZACION DOMINIO:

INFORMACION DE LA INSTITUCION

Nombre Completo:

Siglas:

Dirección Postal

Calle y No.

Colonia

Del o Mpio.

Ciudad

Estado

Codigo Postal

CONTACTO ADMINISTRATIVO:

nic-Handle:

Título:

Nombre(s):

Apellido Paterno:

Apellido Materno:

Puesto:

Email:

Teléfono:

Fax:

COMENTARIOS:

Enviar Limpiar

Última actualización: 01 OCTUBRE 1998 Tel. 622 8119

4.3.2 Políticas de Asignación de Direcciones IP

1.- La solicitud de asignación de direcciones IP deberá hacerse por medio del formato de Web o, en su defecto, través de correo electrónico.

a) Solicitud a través de Web:

- ✓ Ingresar el URL http:// www.nic.unam.mx
- ✓ Ingresar a la liga: Formas de registro
- ✓ Ingresar a la liga: Solicitud de Direcciones IP
  - Dependencias de la UNAM
- ✓ Llenar los campos de la forma de registro con los datos correctos.

b) Solicitud a través de Correo Electrónico:

- ✓ Bajar el formato de texto vía FTP y seguir las instrucciones indicadas al final del archivo:

ftp:// ftp.nic.unam.mx/Formas/DirIP1-Solicitud

2.- Este trámite solo podrá hacerlo los responsables de la red local de la dependencia. Si no se cuenta con acceso a Internet o acceso a Web, como caso especial, los responsables deberán comunicarse vía telefónica con NICunam para indicarles el procedimiento a seguir.

3.- La información contenida en la solicitud será verificada y ratificada de acuerdo a la base de datos de NICunam. En caso de encontrarse información falsa o no congruente, la solicitud será rechazada y se notificará a los responsables de la dependencia y al solicitante.

4.- Las solicitudes serán procesadas de acuerdo al orden en que se reciban.

5.- Si se han asignado direcciones IP previamente a la dependencia, el solicitante deberá incluir una relación completa de la forma en que han sido distribuídas dichas direcciones de acuerdo a como se indica en la solicitud.

En caso de no incluirse esta relación, o que los datos de la misma no estén completos ni actualizados a la fecha, la solicitud será rechazada inmediatamente.

6.- Se deberá anexar los planos esquemáticos de la forma en que están distribuídos físicamente todos y cada uno de los equipos de cómputo que tienen una dirección IP, como está indicado en la solicitud.

Estos planos deberán entregarse antes de la fecha indicada para que la asignación de direcciones IP no sea revocada.

7.- En la forma de solicitud, se deberá incluir la justificación correspondiente indicando el número de direcciones IP solicitadas, así como la planeación correspondiente.

En caso de no incluírse esta justificación, la solicitud será rechazada imediatamente.

8.- Si el solicitante cumple con todos los requisitos se procederá a la asignación de las direcciones IP. El tiempo de asignación depende del tiempo de revisión de la documentación proporcionada por el solicitante; por ello debe de entregarse con las características solicitadas por NICunam.

9.- Una vez asignado el rango de direcciones IP, los responsables de la red serán los encargados de hacer la distribución de las mismas de acuerdo a su planeación y se encargarán de mantener su relación actualizada, así como los planos correspondientes.
10.- NICunam solicitará a los responsables esta información de forma regular. En caso de que los responsables de la red no entreguen la documentación en cuanto se les solicite, se suspenderán los servicios de nombres, dominios y asistencia técnica a la dependencia, hasta el momento en que se entregue dicha documentación.
NICunam, establecerá un periodo de gracia, en caso de no acatarse la disposición de entrega de documentación. Si al concluir este periodo de gracia no se ha entregado la documentación requisitada nuevamente, se procederá a hablar con el director de la dependencia con el fin de recomendarle la nueva asignación de un responsable (o responsables) de Red que cumpla debidamente con sus responsabilidades.

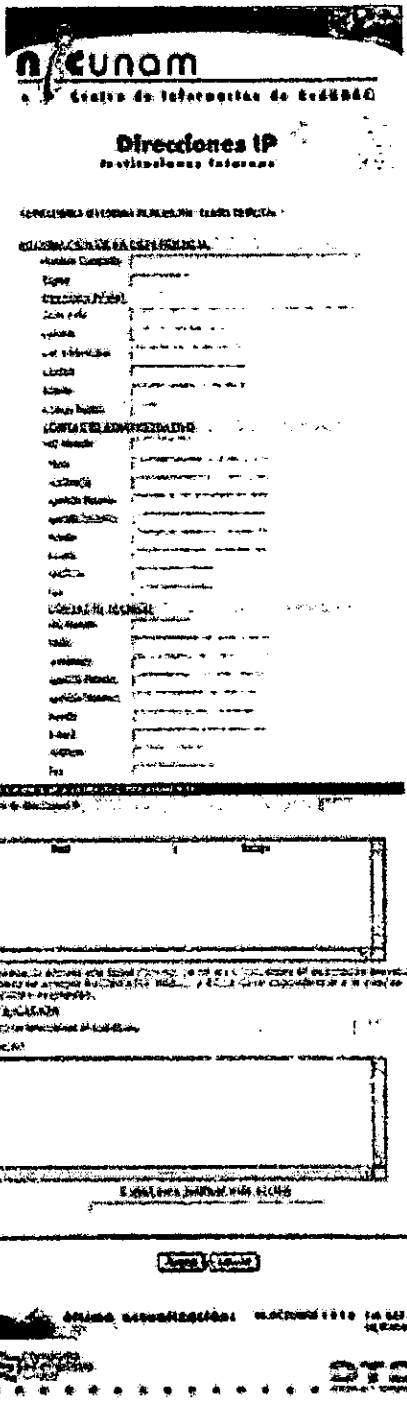
Direcciones IP para Instituciones Conectadas a la UNAM

1.- La solicitud de asignación de direcciones IP deberá hacerse por medio del formato de Web, o en su defecto, a través de correo electrónico.
a) Solicitud a través de Web:
- ✓ Ingresar el URL http://www.nic.unam.mx
- ✓ Ingresar a la liga: Formas de registro
- ✓ Ingresar a la liga: Solicitud de Direcciones IP
  - Instituciones conectadas a la UNAM
- ✓ Llenar los campos de la forma de registro con los datos correctos.

b) Solicitud a través de Correo Electrónico:
- ✓ Bajar el formato de texto vía FTP y seguir las instrucciones indicadas al final del archivo: ftp://ftp.nic.unam.mx/Formas/DirIP2-Solicitud

2.- Este trámite solo podrán hacerlo los responsables de la red local de la Dependencia. Si no se cuenta con acceso a Internet o acceso a Web, como caso especial, los responsables deberán comunicarse vía telefónica con NICunam para indicarles el procedimiento a seguir.
3.- Una vez establecido el vonvenio de conexión con la UNAM, cualquier institución tendrá la opción de solicitar direcciones IP a NICunam para asignar a sus hosts.
4.- Si la institución cuenta con direcciones IP que se le hayan asignado previamente por otras circunstancias y cuya propiedad corresponda a la institución, podrán seguirlas utilizando sin ningún problema. Pero se tendrá que entregar la documentación de esas redes a NICunam de acuerdo a la solicitud.
5.- Si se han asignado direcciones IP previamente a la institución, por parte de NICunam, el solicitante deberá incluir una relación completa de la forma en que han sido distribuídas dichas direcciones de acuerdo a como se indica en la solictud.
En caso de no incluirse esta relación, o que los datos de la misma no estén completos ni actualizados a la fecha, la solicitud será rechazada inmediatamente.

6.- Se debarán anexar los planos esquemáticos de la forma en que están distribuídos físicamente todos y cada uno de los equipos de cómputo que tienen una dirección IP, como está indicado en la solicitud. Así como también planos topológicos de la red a nivel general.
Estos planos deberán entregarse antes de la fecha indicada para que la asignación de direcciones IP no sea revocada.
7.- En la forma de solicitud, se deberá incluir la justificación correspondiente indicando el número de direcciones IP solicitadas, así como la planeación correspondiente.
En caso de no incluirse esta justificación, la solicitud será rechazada inmediatamente.
8.- Si el solicitante cumple con todos los requisitos se procederá a la asignación de las direcciones IP. El tiempo de asignación depende del tiempo de revisión de la documentación proporcionada por el solicitante; por ello debe de entregarse con las características solicitadas por NICunam.
9.- Una vez asignado el rango de direcciones IP, los responsables de la red serán los encargados de hacer la distribución de las mismas de acuerdo a su planeación y se encargarán de mantener su relación actualizada, así como los planos correspondientes.
10.- Las direcciones IP que se proporcionan a las Instituciones conectadas a la UNAM son NO Portables; es decir, en caso de que la Institución requiera desconectarse de RedUNAM para su acceso a Internet, deberá hacer una petición de direcciones IP a su nuevo proveedor y tendrá que reconfigurar sus hosts con las nuevas direcciones IP. No podrá conservar las asignadas por NICunam, quedando éstas a disposición de poder reasignarse a otra Institución.
11.- NICunam solicitará a los responsables esta información de forma regular. En caso de que los responsables de la red no entreguen la documentación en cuanto se les solicite, se suspenderán los servicios de asistencia técnica y servicio de servidor secundario (en caso de tenerlo). Se dará un plazo para la entrega de la información; de no cumplirse, se procederá al retiro de direcciones IP de dicha institución.



4.4 Estructura del DNS

4.4.1 Dominios

El sistema de nombres de dominio dentro de Internet, se basa en la estructura del espacio de nombres de dominio. Esta estructura es de forma arborecente y jerárquica semejante a un sistema de archivos Esta estructura puede tener "n" niveles donde los nodos intermedios representan dominios o subdominios, y los nodos finales, generalmente representan los nombres de los hosts.
Los Top Level Domain son asignados por InterNIC, mientras que los dominios del tercer nivel en adelante son asignados y delegados de acuerdo a los registros regionales y a los propietarios de los mismos.
En el caso de los dominios bajo MX, estos son delegados y asignados por NIC-México; a su vez, los dominios bajo UNAM-MX son asignados por NICunam. Algunos dominios de este tipo son:

nic.unam.mx
dgsca.unam.mx
fciencias.unam.mx
donde los hosts tienen como nombre, por ejemplo:

www.nic.unam.mx
servidor.dgsca.unam.mx
hp.fciencias.unam.mx

4.4.2 Servidores de Nombres

Actualmente RedUNAM cuenta con cuatro servidores de nombres encargados de la resolución de diversos dominios, principalmente UNAM.M:

dns1.unam.mx	☞	132.248.204.1	☚	Nodo DGSCA
dns2.unam.mx	☞	132.248.10.2	☚	Nodo DGSCA
dns3.unam.mx	☞	132.248.64.250	☚	Nodo IIMAS
dns4.unam.mx	☞	132.248.237.250	☚	Nodo Zona-Cultural

Esto servidores son administrados y operados única y exclusivamente por el Centro de Información de RedUNAM (NICunam). Estos equipos están corriendo la versión 8.1.1 de BIND y están distribuídos de forma topológica en RedUNAM. El orden recomendado para configurar en los hosts los posibles servidores de nombres es:

a) Si la red depende del Nodo DGSCA:

132.248.10.2

132.248.204.1
132.248.64.250
132.248.237.250

b) Si la red depende del Nodo IIMAS:

132.248.10.2	132.248.64.250
132.248.64.250	132.248.10.2
132.248.237.250	132.248.237.250
132.248.204.1	132.248.204.1

c) Si la red depende del Nodo ZONA-CULTURAL

132.248.10.2	132.248.237.250
132.248.237.250	132.248.10.2
132.248.64.250	132.248.64.250
132.248.204.1	132.248.204.1

Actualmente existen una gran cantidad de dominios bajo UNAM.MX, los cuales corresponden a las siglas o nombres de las dependencias de la UNAM. Así por ejemplo, tenemos el caso de:

FCIENCIAS.unam.mx	Facultad de Ciencias
DGSCA.unam.mx	Dirección General de Servicios de Cómputo Académico
FI-P	Facultad de Ingeniería, Edificio de Posgrado

También existe el caso del servidor ns.nic.unam.mx, el cual es el encargado de hacer la función de servidor secundario para el dominio MX.
Éste servidor es el único que se encuentra fuera de la administración de NIC-México, encargándose de ésto NICunam. Éste servidor se ubica en el Nodo de Zona Cultural.

Características de los servidores

dns1.unam.mx

Este servidor es una SPARCstation 4 con un disco duro de 1.05 GB, 64 MB de memoria y trabaja con el sistema operativo Solaris 2.5.1 - SunOS 5.5.1.

Es el servidor primario para el dominio unam.mx, en él se encuentran:

- Dominios de la UNAM (dominios internos)
- Dominios de Instituciones que tienen Alojo de Servidores
- Algunos dominios de Instituciones Conectadas que desean que dns1 sea su servidor de nombres primario.

- Dominios para el Alojo de páginas.
- Dominios Inversos de la UNAM
- Dominios Inversos de las Instituciones Conectadas a excepción de aquellos dominios que sean de la red X.15.200.in-addr.arpa

dns2.unam.mx

Este servidor es una SPARCstation 4 con un disco duro de 1.05 GB, 64 MB de memoria y trabaja con el sistema operativo Solaris 2.5.1 - SunOS 5.5.1.

Es servidor secundario para el dominio unam.mx, en él se encuentran:

- Dominios de la UNAM (dominios internos)
- Dominios de Alojo de Servidores
- Algunos dominios de las Instituciones Conectadas que desean que dns1 sea el servidor de nombres primario.
- Dominios para el alojo de páginas
- Dominios Inversos de la UNAM
- Dominios Inversos de las Instituciones Conectadas a excepción de aquellos dominios que sean de la red X.15.200.in-addr.arpa
- Dominios de Instituciones Conectadas en donde se desea que dns2 funja como servidor de nombres secundario.

dns3.unam.mx

Este servidor es una SPARCstation 2 con un disco duro de 424 MB, 64 MB de memoria y trabaja con el sistema operativo Solaris 2.5.1 - SunOS 5.5.1.

Es servidor secundario para el dominio unam.mx, en él se encuentran:

- Dominios de la UNAM (dominios internos)
- Dominios de Instituciones que tienen Alojo de Servidores
- Algunos dominios de Instituciones Conectadas que desean que dns1 sea su servidor de nombres primario.
- Dominios para el Alojo de páginas.
- Dominios Inversos de la UNAM
- Dominios Inversos de las Instituciones Conectadas a excepción de aquellos dominios que sean de la red X.15.200.in-addr.arpa

dns4.unam.mx

Este servidor es una SPARCstation LX con un disco duro de 424 MB, 64 MB de memoria y trabaja con el sistema operativo Solaris 2.5.1 - SunOS 5.5.1.

Es servidor secundario para el dominio unam.mx, en él se encuentran:

- Dominios de la UNAM (dominios internos)
- Dominios de Instituciones que tienen Alojo de Servidores
- Algunos dominios de Instituciones Conectadas que desean que dns1 sea su servidor de nombres primario.
- Dominios para el Alojo de páginas.
- Dominios Inversos de la UNAM
- Dominios Inversos de las Instituciones Conectadas a excepción de aquellos dominios que sean de la red X.15.200.in-addr.arpa

ns.unam.mx

Este servidor es una SPARCstation 4 con un disco duro de 1.05 GB, con 32 MB de memoria y trabaja con el sistema operativo Solaris 2.5.1 - SunOS 5.5.1.
Este servidor tiene asignada la dirección IP 132.248.253.1, y como ya se menciono es servidor secundario para el dominio MX.

Diariamente a las 12:00 de la noche corre un programa en cada uno de los servidores, el cual se encarga de hacer un respaldo diario de cada uno de los archivos del directorio NAMED, que corresponden a cada uno de los dominios para los que resuelven los cuatro servidores de nombres. También corren otros programas, que se encargan de obtener el estado de cada uno de ellos, así como también el verificar si existe algún problema en sus archivos.
En cada uno de los servidores, se ha instalado software de seguridad a fin de evitar que tengan acceso a ellos personas ajenas al NICunam. Entre estas medidas de seguridad se ha instalado el TCP Wrapper y el Secure Shell.

Para todas las instituciones de la UNAM, así como para aquellas empresas que tienen alojo de servidores en la UNAM, los únicos servidores de nombres oficiales son dns1.unam.mx, dns2.unam.mx, dns3.unam.mx y dns4.unam.mx, ya que NICunam se encarga de administrar todos los dominios inversos, por lo que para seguir manteniendo una consistencia en la Base de Datos se prohibe tener otros servidores de nombres.
Para los dominios que se encuentran bajo la red x.15.200.in-addr.arpa se deben dar de alta ante SESQUINET y uno de sus servidores secundarios debe ser: ns.sesqui.net. Esto se debe a que la red 200.15.X es de SESQUINET, pero le brindó a la UNAM una parte de su administración, por lo que la asignación de direcciones IP bajo esta red la hace NICunam, pero la asignación inversa la hace SESQUINET como ya se mencionó.

Para la red 3.15.200.in-addr.arpa y la 12.15.200.in-addr.arpa los servidores de nombres oficiales son dns1.unam.mx, dns2.unam.mx, dns3.unam.mx, dns4.unam.mx y ns.sesqui.net.

4.4.3 Solicitudes para altas, bajas y cambios en el DNS

Bajo cada uno de los dominios ya sea de dependencias de la UNAM o externas, existen unas serie de nombres y asociaciones que nos permiten manejar la comunicación entre hosts de una forma más amigable para el ser humano, entre los que se encuentran:

- Nombres Canónicos
- Alias
- Mail Exchangers

los cuales ya se describieron en el capítulo 2.

◎ Solicitud de altas y bajas

1.- Las solicitudes de altas y bajas para el DNS deberán hacerse por medio del formato de Web o, en su defecto a través de correo electrónico.

a) Solicitud a través de Web:
   - ✓ Ingresar el URL: http://www.nic.unam.mx
   - ✓ Ingresar a la liga: Formas de Registro
   - ✓ Ingresar a la liga: Servicio de Nombres de RedUNAM

   Llenar los campos de la forma de registro con los datos correctos.

b) Solicitud a través de Correo Electrónico:
   - ✓ Bajar el formato de texto vía FTP y seguir las instrucciones indicadas al final del archivo: ftp://ftp.nic.unam.mx/Formas/DNS-Solicitud

2.- En la solicitud de altas y/o bajas solo se pueden hacer mención a un solo dominio. En caso de que la solicitud venga asociada a más de uno, no podrá ser procesada.

3.- El dominio al cual esté asociada la solicitud deberá existir; esto significa que el dominio deberá haber sido dado de alta previamente antes de solicitar alguna alta o baja sobre él.

4.- Estas solicitudes serán procesadas siempre y cuando la dirección de correo indicada en la solicitud corresponda a:

- ✓ E-Mail Exchanger del Responsable Administrativo del dominio
- ✓ E-Mail Exchanger del Responsable Técnico del dominio
- ✓ E-Mail Exchanger de Staff para el dominio

5.- Las solicitudes serán procesadas de acuerdo al orden en que se reciban.

6.- Al hacer la solicitud:

a) En caso de requerir varios movimientos (altas o bajas) por cada uno de los tipos de registros (hosts, alias, mail exchangers), estos se deberán listar de manera ascendente de acuerdo a la dirección IP.

b) Solo se aceptarán un número máximo de altas o bajas por cada tipo de movimientos en las solicitudes:

Hosts

Altas <= 50
Bajas <= 50

Alias

Altas <= 15
Bajas <= 15

Mail Exchangers

Altas <= 15
Bajas <= 15

c) En Mail Exchangers, la asignación de prioridades deberá ser de manera consecutiva siempre empezando desde 0. La prioridad puede ser igual para 2 o más mail exchangers.
d) Para Mail exchangers, la solicitud de alta en el DNS es necesaria, más no suficiente para que el servicio de correo relativo al mail exchanger funcione adecuadamente. Para ello debe estar configurado adecuadamente el o los hosts que harán esta función.

7.- Para solicitar modificaciones a las Bases de Datos de los servidores de nombres de la UNAM solo se puede recurrir a dos tipos de movimientos: Altas y/o Bajas. Los cambios no están permitidos de manera directa; la forma alternativa de realizarlos es mediante Bajas y Altas de los registros.
8.- Un vez procesada la solicitud por personal de NICunam, se enviará por correo electrónico la notificación correspondiente al solicitante.
9.- Tanto el responsable administrativo como técnico deberán conocer y respetar estas políticas, haciéndolas del conocimiento de todos sus usuarios.

CASOS ESPECIALES:

1.- Cuando se requiere un alias, éste deberá pertenecer al dominio; pero podrá estar asociado a un nombre canónico de cualquier otro dominio, siempre y cuando el nombre canónico del host pertenezca a cualquiera de los dominios de la UNAM. En este caso no es requisito ser el responsable del dominio del host al cual este asociado el alias; sin embargo, es indispensable que las personas encargadas del dominio tengan conocimiento de esta solicitud. (Este caso no aplica a usuarios y/o dominios ajenos a UNAM.MX)
2.- En el caso de los Mail Exchangers, el nombre o dominio para el cual se requieran, deberá pertenecer al dominio al cual hace referencia la solicitud. Al igual que los alias, los mail exchangers pueden tener un nombre canónico que se encuentre en otro dominio de la UNAM; pero es necesario que los responsables de los dominios de los mail exchangers están al tanto de dicha solicitud.
3.- Las altas y bajas de hosts bajo el dominio unam.mx no se permiten, los únicos movimientos que se permiten bajo este dominio son altas y/o bajas de alias y mail exchangers, siempre y cuando se anexe la justificación breve y concisa.

nicunam

Centro de Información de RedUNAM

Servicio de Nombres de RedUNAM

| [illegible] | [illegible] |

[illegible] **Solicitud del Servicio de DNS** [illegible] [illegible]

[illegible] **políticas de uso para el DNS de RedUNAM**.

DATOS DEL SOLICITANTE

Nombre: ____________________

E-mail: ____________________

[Responsable Técnico ▾]

Dominio: [illegible].unam.edu / unam.mx / acatlan.unam.mx / [illegible].unam.mx

Nota: [illegible]

Favor de indicar el número de movimientos que se deseen:

	HOSTS	ALIAS	MAIL EXCHANGERS
Altas			
Bajas			

[Continuar] [Limpiar]

Última actualización: [illegible] OCTUBRE [illegible] Tel. [illegible]
[illegible]

Cómputo Académico UNAM — DTD DGSCA - UNAM

4.4.4 Archivos de configuración y Base de Datos de los servidores de nombres

Debido a que los cuatro servidores de nombres de la UNAM corren la versión 8.1.1 de BIND, el archivo de configuración no lleva por nombre named.boot, sino que se le conoce como named.conf, el cual se localiza en el directorio /etc.

Archivo de configuración named.conf

Este archivo se compone de las siguientes partes:

- Opciones
- Loggings
- Zonas
  - Master (master)
  - Esclavo (Slave)

Options: Especifica los aspectos globales de la operación del servidor de nombres.

```
options {
        directory " ruta del directorio que contiene lo archivos de la Base de Datos (named) "
        named-xfer " Programa que se encraga de realizar la transferencia de las tablas desde los
        servidores de nombres remotos "
        dump-file " Archivo en donde se efectúa el respaldo de la base de datos interna del servidor de
        nombres cuando recibe la señal INT "
};
```

Logging: Se encarga de efectuar un registro de cada evento que ocurre en el DNS. Se pueden realizar estadísticas, consultas, errores, etc. A cada una de estas categorías o eventos se les conoce como canales.

Zonas: Se definen las características de cada zona.

- Master.- Hace referncia de los datos en una zona primaria.

```
zone " Nombre del dominio" {
        type master;
        file " Archivo en donde se encuentran las tablas ";
        };
```

- Slave.- Una zona esclava es una copia de una zona master, a la que comúnmente se le conoce como secundaria.

```
zone " Nombre del dominio" {
        type slave;
```

```
            file " Archivo en donde se encuentran las tablas ";
            masters { IP del servidor de nombres primario ;
            };
};
```

Ejemplo del archivo named.conf del servidor de nombres primario dns1.unam.mx (por razones de seguridad solo se presenta una parte).

```
# SERVIDOR PRIMARIO dns1.unam.mx [132.248.204.1]
#
# Last Update [yymmddss]: 99102900
# Modificado por      : jamm

options {
    directory "/home/named";
    named-xfer "/usr/local/sbin/named-xfer";
    dump-file "/tmp/named/server/named.dump";
    allow-query {
        any;
    };
    allow-transfer {
        any;
    };
    notify yes;
};

logging {
    channel default1-chn {
        file "/tmp/named/category/default-critical"
        versions 2
        size 1048576;
        severity critical;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    channel default2-chn {
        file "/tmp/named/category/default-error"
        versions 2
        size 1048576;
        severity error;
        print-category yes;
```

```
        print-severity yes;
        print-time yes;
    };
    channel default3-chn {
        file "/tmp/named/category/default-warning"
        versions 2
        size 1048576;
        severity warning;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    channel default4-chn {
        file "/tmp/named/category/default-notice"
        versions 2
        size 1048576;
        severity notice;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
.
.
.
.
.
zone "127.in-addr.arpa" {
    type master;
    file "named.127";
};

# SUBDOMINIOS UNAM.EDU
# ====================

# Servidores:  132.248.204.1
#              132.248.10.2

zone "unam.edu" {
    type master;
    file "named.unam.edu";
};
```

```
zone "usa.unam.edu" {
      type master;
      file "named.usa.unam.edu";
};
.
.
.
.
```

Ejemplo del archivo named.conf del servidor de nombres secundario dns2.unam.mx (por razones de seguridad solo se presenta una parte).

```
#  SERVIDOR SECUNDARIO dns2.unam.mx [132.248.10.2]
#
#  Last Update [yymmddss]: 99102900
#  Modificado por       : jamm

options {
      directory "/home/named";
      named-xfer "/usr/local/sbin/named-xfer";
      dump-file "/tmp/named/server/named.dump";
      allow-query {
            any;
      };
      allow-transfer {
                  132.248.10.2;
                  132.248.64.250;
                  132.248.237.250;
      };
      notify yes;
};

logging {
      channel default1-chn {
            file "/tmp/named/category/default-critical"
            versions 2
            size 1048576;
            severity critical;
            print-category yes;
            print-severity yes;
            print-time yes;
      };
```

```
    channel default2-chn {
        file "/tmp/named/category/default-error"
        versions 2
        size 1048576;
        severity error;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    channel default3-chn {
        file "/tmp/named/category/default-warning"
        versions 2
        size 1048576;
        severity warning;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    channel default4-chn {
        file "/tmp/named/category/default-notice"
        versions 2
        size 1048576;
        severity notice;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
.
.
.
.
.
zone "127.in-addr.arpa" {
     type master;
     file "named.127";
};

# SUBDOMINIOS UNAM.EDU
# ====================

# Servidores:  132.248.204.1
#              132.248.10.2
```

```
zone "unam.edu" {
        type slave;
        file "named.unam.edu";
        masters{
                132.248.204.1;
        };
};
zone "usa.unam.edu" {
        type slave;
        file "named.usa.unam.edu";
        masters{
                132.248.204.1;
        };
};
.
.
.
.


# ------------------------------------------------------
#               SERVICIO DE SERVIDOR SECUNDARIO
# ------------------------------------------------------

# DOMINIOS
# ========

zone "asf.edu.mx" {
        type slave;
        file "named.asf.edu.mx";
        masters {
            200.15.128.250;
        };
};

zone "cadi.gob.mx" {
        type slave;
        file "named.cadi.gob.mx";
        masters {
            200.15.38.10;
        };
};
```

```
zone "camaradiputados.gob.mx" {
      type slave;
      file "named.camaradiputados.gob.mx";
      masters {
            200.15.38.10;
      };
};
```

Ejemplo de un archivo de la Base de Datos del servidor de nombres dns1.unam.mx (por razones de seguridad solo se presenta una parte).

Archivo named.unam

```
;
; RR SOA Start of Authority
; ------------------------
;
@     IN    SOA    dns1.unam.mx.        dns.unam.mx. (
                  99102700              ; Serial  [yymmddss]
                  3600                  ; Refresh [secs]
                  1200                  ; Retry   [secs]
                  1814400               ; Expire  [secs]
                  7200 )                ; TTL     [secs]
;
; RR NS Name Servers
; ------------------
;
      IN    NS    dns1.unam.mx.
      IN    NS    dns2.unam.mx.
      IN    NS    dns3.unam.mx.
      IN    NS    dns4.unam.mx.

;
; RR MX Mail Exchangers
; ---------------------
;
                  IN    MX    1     deimos.nic
tel98             IN    MX    0     deimos.nic
beta-site         IN    MX    0     deimos.nic
cefini            IN    MX    0     uxmal.cifn
n2.cefini         IN    MX    0     uxmal.cifn
redunam           IN    MX    0     helpdesk.dgsca
```

```
ifunam          IN    MX    0     fenix.ifisicacu
cisan           IN    MX    0     cisan.laborales

;
; RR A Name-to-Address Mapping
; ------------------------------
;
@               IN    A     132.248.204.6
servidor        IN    A     132.248.10.1
dns2            IN    A     132.248.10.2
servidor        IN    A     132.248.10.4
servidor        IN    A     132.248.10.5
dns3            IN    A     132.248.64.250
dns1            IN    A     132.248.204.1
dns4            IN    A     132.248.237.250
ns              IN    A     132.248.253.1

;
; RR CNAME Canonical Name (Alias)
; -------------------------------
;
www.artesvisuales   IN    CNAME   argon.servidores
www.pdcb            IN    CNAME   pdcb.biomedicas
cch.vallejo         IN    CNAME   www.cch-vallejo
cch2.vallejo        IN    CNAME   www2.cch-vallejo
www.csa             IN    CNAME   www.coseac
wwwaime             IN    CNAME   fufimat5.cuautitlan2
webforce            IN    CNAME   fufimat2.cuautitlan2
sunsite             IN    CNAME   sunsite.dcaa
www.prometeo        IN    CNAME   prometeo.dgae1
www.ddu             IN    CNAME   cakes.dgasc
alianza             IN    CNAME   vasconcelos.dgsca
```

CONCLUSIONES

Al pensar en nuestra civilización, no es posible dejar a un lado el mundo de la computación, ahora todo o casi todo funciona o se maneja por medio de estos equipos; desde una simple computadora para llevar inventarios o estadísticas en una pequeña oficina o realizar trabajos escolares, hasta sofisticadas supercomputadoras que se encargan de manejar o dirigir el funcionamiento de grandes maquinarias o realizar cálculos que para el hombre serían imposibles de llevar a cabo por otros medios. Pensar en un mundo sin computadoras, tal vez hoy, suena imposible.

Así como se va incrementando la importancia de las computadoras día con día, el mundo de Internet se va desarrollando en el mismo sentido. Ahora cualquier empresa, ya sea chica, mediana o grande, empresas nacionales o transnacionales, utilizan el mundo de Internet para comprar, llevar a cabo sus promociones, vender sus productos, o simplemente mostrar información de algún tipo, ya sea de carácter político, económico, militar, educativo o solo de diversión.

¿Pero que hay detrás de Internet? ¿Qué es lo que la hace funcionar? Muy pocas personas se han preguntado que existe detrás de este término tan usado en la actualidad. No es solo escribir una dirección en algún navegador, para obtener como por arte de magia, la información requerida. Existe todo un mundo de equipos y sistemas que trabajan en forma transparente para que el usuario común pueda hacer de Internet su herramienta de trabajo o esparcimiento diaria. Uno de los sistemas fundamentales para que la búsqueda y transporte de información sea transparente y amigable para las personas, es el DNS.

Usualmente la importancia del DNS es subestimada, incomprendida o ignorada. La realidad es que sin el DNS casi ningún servicio de Internet sería funcional: el correo electrónico, la transferencia de archivos anónima, el WWW, etc. ¿Por qué? Simplemente porque el DNS es el sistema que sirve de intérprete entre las nomenclaturas técnicas de direcciones IP, mail exchanger y similares, a un "vocabulario" común, capaz de ser entendido, recordado e incluso intuido por una persona sin necesidad de comprender toda la complejidad técnica de Internet. La gente no sería capaz de recordar una serie de números sin sentido: 132.248.10.4 para su correo electrónico, 132.248.204.49 para el ftp anónimo, 132.248.10.10 para el WWW, etc.; una serie de números no puede ser tan representativa o expresiva como tener servidor.unam.mx para el correo o www.unam.mx para el WWW. El empleo de nombres en lugar de números nos da un indicio del servicio que estamos utilizando así como la institución y país desde donde lo estamos solicitando. Es sumamente fácil escribir www.unam.mx sin saber de antemano si ésta existe o no, pero es partir de algo intuitivo o conocido, a diferencia de intentar localizar un servicio por medio de una dirección IP.

Gracias a la facilidad de relacionar un nombre a una dirección IP, Internet ha llegado a ser lo que es ahora, pero este mapeo básico de direcciones IP's a nombres no es tan simple, detrás de esta operación tan sencilla para el usuario, existen servicios mas complejos o sofisticados. Ejemplo de éstos son el uso de mail exchangers o simplemento los servidores de DNS. Es por esto que consideré importante realizar un trabajo donde se describiera el funcionamiento del DNS y con ello se pudiera comprender mejor su importancia para la correcta operación de casi la totalidad de los servicios de Internet, además de documentar los procedimientos administrativos necesarios para lograr que la operación de un sistema tan importante como el DNS sea ágil, confiable y eficiente.

NICunam surge como administrador de los servidores de nombres de la RedUNAM, así como de los nombres de dominio que se encuentran bajo UNAM.MX. La importancia del NICunam tal vez pase desapercibida para muchas personas, pero el correcto funcionamiento de esta área es fundamental para la operación de la red; no todos los problemas en la red son en los equipos de transporte o de ruteo, también pueden surgir graves problemas si no se sigue un estricto control en la asignación de direcciones IP y sus respectivos nombres, actividades que son coordinadas por el NICunam.

El administrar un sistema de nombres de dominio o DNS es una tarea delicada, ya que un error en la configuración de sus archivos puede ocasionar serios problemas. El presente trabajo, pretende acotar parte de los procesos de dicha administración: las bases técnicas y la documentación de los procedimientos existentes. En las bases técnicas no sólo se desarrollan los conceptos concernientes a la operación de los servidores de nombres sino que también se retomaron las herramientas y procedimientos de identificación y resolución de fallas en el DNS, procurando que con esto más personas puedan entender y colaborar en la correcta operación del servicio de nombres de la UNAM. Como el proyecto cultural más importante de la nación, la UNAM se encuentra en continuo desarrollo y el cómputo y las telecomunicaciones no son la excepción. Sin embargo este desarrollo ha implicado que en más de una ocasión los procesos de documentación se deleguen a segundo término, no obstante su importancia; este trabajo retoma esta importante tarea para comprender mejor en donde estamos, como trabajamos, hacia donde nos dirigimos y como podemos lograrlo.

BIBLIOGRAFÍA

Albitz, Paul, Liu, Cricket. DNS and BIND. U.S.A., O'Reilly & Associates, INC., 1992.

Black Uyless. Redes de ordenadores. Protocolos, normas e interfaces. España, RA-MA, 1994.

Black Uyless. TCP/IP and Related Protocols. U.S.A., Mc Graw Hill, 1994.

Craig, Hunt. TCP/IP. Network Administration. U.S.A., O'Reilly & Associates, INC., 1992.

Douglas, E. Comer. Redes Globales de información con Internet y TCP/IP. México, Prentice Hall, 1996.

Harley, Hahn. INTERNET. Manual de Referencia. España, Mc Graw Hill, 1994.

Feit, Sidnie. TCP/IP. U.S.A., Mc Graw Hill, 1993.

OTRAS REFERENCIAS

http://www.nic.unam.mx

http://www.nic.mx

http://www.khainata.com/extrainternet/int.html

http://www.maznam.msctm.net.my/course/one/freesoft/CIE/Topics/35.htm

http://clients.servint.com/network/nslookup.html

http://sunsite.net.edu.cn/tutorials/NetworkingGuide/dnsC.nslook.html

http://www.nodo50.org/manuales/internet/3.htm

http://www.vc.ehu.es/wuagacaj/manual/glosario/indice-d.html

http://www.eusnet.org/ayuda/herramientas/mac/tdominio.htm

http://osiris.staff.udg.mx/man/internet/capitulo1.html

http://www.sedet.com.mx/conexiones/hisint.html

http://www.ontinyent.com/juanypaco/internet.htm

http://www.ontinyent.com/juanypaco/funciona.htm

http://www.geocities.com/SiliconValley/Bay/8259/contenido.html

http://www,lmu.edu/admin/IS/training/protected/tcpip.html

http://www.pucp.edu.pe/ricpucp/servint.interhisto.html