UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

"PRÀCTICAS DEL PROTOCOLO TCP/IP PARA UN LABORATORIO DE REDES AN LA ENEP ARAGÓN"

T E S I S

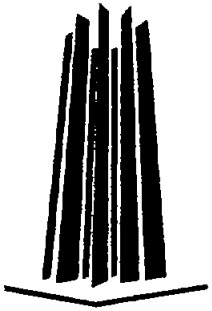
QUE PARA OBTENER EL TITULO DE:

INGENIERA EN COMPUTACIÓN

P R E S E N T A N:

MAYRA GEORGINA PINEDA SANDOVAL

SILVINA DE LA LUZ JIMÉNEZ GÒMEZ



ASESOR: ING. JOSE MANUEL QUINTERO CERVANTES

SAN JUAN DE ARAGÓN, ESTADO DE MEXICO

[redacted] 2005

Agradecemos a:

La **Universidad Nacional Autónoma de México** por forjar nuestra educación y habernos albergado durante todos estos años, donde aprendimos el valor del conocimiento, el valor de la amistad y el valor de la lealtad.

A nuestro asesor **Ing. José Manuel Quintero Cervantes** por dirigir este trabajo de tesis, por su paciencia y dedicación, por sus consejos y exhortaciones, pero sobre todo por su amistad sincera.

A la **Escuela nacional de Estudios Profesionales plantel Aragón y profesores** de la carrera de Ingeniería en Computación por su contribución con nuestra formación académica.

A nuestros **amigos** de la carrera, por su apoyo y su ayuda cuando la necesitamos, por cada cosa que aprendimos de cada uno de ellos.

Mayra Georgina Pineda Sandoval

Esta tesis la dedico con todo mi amor y cariño.

A ti Dios que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papá y mamá, por haberme dado las herramientas necesarias para terminar mi carrera y por creer en mí. Gracias por su ejemplo y por los valores que me han inculcado. Aprovecho este espacio para decirles que los amo y que son mi mejor ejemplo de vida a seguir.

A mis hermanas Alejandra y Bety, porque aún cuando las diversas circunstancias hacen que no podamos estar juntas, he contado con su apoyo y cariño, las quiero mucho.

A mi chiquita, por ser una de mis más grandes alegrías

A Guillermo Reyes Correa por apoyarme en cada momento, por su amor y comprensión, por su paciencia y tolerancia. También aprovecho este espacio para decirte que te amo mucho y eres una de las personas más importantes en mi vida.

A mis amigos de la carrera, por su amistad desinteresada y por su ayuda cuando la necesite. En especial a dos amigos (que no es necesario mencionar su nombre) que siempre estuvieron en momentos muy difíciles, que cuando sentía que ya nada valía la pena ellos estuvieron siempre dispuestos a brindarme su ayuda, su apoyo y sobre todo su cariño y comprensión.

A Silvina de la Luz Jiménez Gómez, porque juntas logramos realizar este trabajo, gracias por el apoyo brindado y su amistad.

A Vicky por su apoyo y comprensión.

A Cristina y Francisco por su amistad y cariño, y por estar siempre al pendiente de mí.

A Gude, Poncho, Soco, Mario, Fer y Roy por su amistad y por sus oraciones.

A la Universidad Nacional Autónoma de México, por ser la mejor y más grande casa de estudios de México y América Latina.

Es la hora de partir, la dura y fría hora que la noche sujeta a todo horario...
(PabloNeruda)

Silvina de la Luz Jiménez Gómez

A Dios
Por darme la vida y permitir que alcance esta meta.

A mi Madre, Norma Gómez
Porque con su amor, cariño, confianza y dulzura me lleva siempre por el camino de la superación y excelencia, y por escalar junto a mi cada peldaño de mi vida. Gracias por tus consejos. Te amo.

A Norma Ruth, Mónica Erendira, Gabriela Montserrat, Javier y David de Jesús
Por su apoyo incondicional, ayuda y amor que me dan día a día. Gracias por estar a mi lado.

A Tío Juan
Por su amor y su alegría.

A Luz Andrea
Por su amor y su compañía.

A Luis Javier
Por su cariño y ternura.

A Héctor Octavio
Por su amor, apoyo, confianza, y su interés en mí.

A Alicia Huerta, Juan Saldaña, Oscar Andrés, Francisco Rodríguez
Por su amistad sincera, una de sus principales virtudes y por su interés en mí.

A Mayra Georgina
Por haber tomado juntas este camino, pero sobre todo por su gran y valiosa amistad.

Los amo a todos.

A mi asesor Ing. José Manuel Quintero Cervantes
Por su amistad, confianza, paciencia y tiempo, mi más sincero
Agradecimiento, ya que su ayuda y dirección fue vital para elaborar el presente trabajo.

Al M. en C. David Moisés Terán Pérez, Ing. Efrén Guerrero Santamaría, Ing. Enrique García Guzmán y al Ing. Ricardo Gutiérrez Orozco
Por toda su ayuda comprensión y por todos sus sabios consejos.

Al M. en C. Marcelo Pérez Medel
Por su apoyo e interés en este trabajo.

A Rodolfo
Por su interés y amistad.

A Vicky
Por la ayuda, tiempo y comprensión que me brindo.

A la Universidad Nacional Autónoma de México
Y en particular a la Escuela Nacional de Estudios Profesionales Aragón
Por la formación profesional y por todo aquello que recibí en sus aulas.

Este trabajo lo dedico a mi Padre, Prof. Javier Jiménez Gómez

Por haberme amado, por haberme comprendido y porque siempre confió en mi. Por haberme inculcado el interés de la superación y por haberme enseñado tantas cosas. Te amo y te extraño.

Dice el maestro:

Querido discípulo, he de darte una noticia
que tal vez todavía no sepas. Pensé en suavizarla,
en pintarla de colores más brillantes, llenarla
de promesas del Paraíso, visiones de lo Absoluto,
explicaciones esotéricas pero, aunque todo eso exista,
no viene ahora al caso.
La noticia es la siguiente: vas a morir.
Puede ser mañana, o dentro de cincuenta años,
pero, tarde o temprano, vas a morir. Aunque no
estés de acuerdo. Aunque tengas otros planes.
Piensa cuidadosamente lo que vas a hacer hoy.
Y mañana. Y el resto de tus días.

Paulo Coelho

Índice

INTRODUCCIÓN

Los autores especializados han dividido la evolución de la humanidad en grandes etapas que han asociado a ciertos fenómenos que denominan revoluciones: agrícola, que hizo al hombre sedentario y le permitió establecerse; industrial que magnificó sus capacidades físicas. En ese sentido se estaría dando ahora la revolución de la información que potencia su inteligencia y sus procesos mentales.

Hacia la década de los 40s del siglo pasado la humanidad se preparaba para un salto gigantesco en su evolución: la era de la información y del conocimiento. A mediados de la década surgieron los primeros sistemas de cómputo, y como otros tantos inventos, sirvieron principalmente para fines militares. En los albores de la siguiente década el hombre descubrió el potencial de los sistemas de cómputo al aplicarlos en los ámbitos civil y comercial.

Durante los siguientes veinte años el uso y explotación de los sistemas de cómputo era privilegio de las grandes empresas, los gobiernos, algunas universidades e instituciones no lucrativas (principalmente en los países ricos y desarrollados). A mediados de los años 70, la tecnología del micro miniaturización había hecho posible que se fabricara un procesador completo en un chip o microcircuito, al que se denominó microprocesador. Este avance tecnológico permitió que un dentista concibiera la idea de un sistema de cómputo completo de uso personal y que al poco tiempo se convirtieran en las computadoras personales como la PC de IBM, entre otras.

Las computadoras de uso personal pusieron los sistemas de cómputo al alcance de las mayorías como usuarios directos, dando un gran impulso a la revolución de la información. Ya la gente podía procesar, almacenar y distribuir su propia información.

A mediados de los 70's, el gobierno de los Estados Unidos de Norteamérica autorizó al Departamento de la Defensa crear una red de grandes sistemas de cómputo interconectados a prueba de bombardeos y que garantizara la información para la toma de decisiones en el ejército estadounidense, a esta red se le llamó ARPANET (Advanced Reserch Projects Agency Network). La comunidad científica y académica se enteró de la existencia de la red y sus posibilidades de comunicación, ya que participaba en diversos proyectos de investigación para el Departamento de la Defensa. Algunas universidades solicitaron permiso y facilidades al gobierno para conectarse a la red y aprovechar sus facilidades y recursos. En muy poco tiempo se agregaron muchos usuarios y así surgió una de las maravillas inventadas en el siglo XX: la Internet.

LA EDUCACIÓN EN LA ACTUALIDAD

El modelo educativo anterior a lo que llamamos la revolución de la información, se caracterizaba por ser autoritario, solo el profesor sabía y tenía la verdad de las cosas.

Didácticamente, era memorista, muy limitado en recursos (pizarrón y gis, libros, cuadernos, lápiz, bibliotecas, etc.) Sus técnicas de enseñanza con frecuencia se basaban en el terror de los escolares con amenazas y consignas en la escuela y el hogar (con sangre la letra entra y otras) y aunque daba buenos resultados en muchos casos, se ha visto que realmente no era lo mejor. Las tecnologías de la información han impactado fuertemente la educación, coadyuvando a crear nuevos modelos educativos en los que se pretende que el alumno aprenda a investigar y construya el conocimiento de manera más eficiente.

Desde el punto de vista tecnológico, actualmente los alumnos de todos los niveles escolares pueden contar con los recursos de las tecnologías de la información para realizar sus estudios. La digitalización hace posible que un disco compacto contenga prácticamente una enciclopedia completa, incluyendo el software para explorarla, con algoritmos de búsqueda muy eficientes y las facilidades para que el usuario pueda copiar las partes que le interesen o imprimirlas. Internet por su parte, facilita la búsqueda y el acceso a un universo virtualmente infinito de información.

El sistema educativo en nuestro país enfrenta un gran problema, porque mientras los estudiantes de otros países aprenden apoyados en las tecnologías de la información, nuestros estudiantes de las escuelas públicas presentan un serio retraso, que necesariamente se verá reflejado en el desarrollo de sus estudios posteriores o en su desarrollo profesional.

La importancia que tienen los métodos de enseñaza en las Universidades es de notable importancia ya que de ésta depende su buen desempeño en el ámbito profesional y al estar aplicando sus conocimientos dentro de una empresa.

Esta tesis muestra las diferentes metodologías de enseñanza de algunas Universidades en México en específico de la materia de Redes de Computadoras y a través de este estudio se plantea la necesidad de implantar un laboratorio de Redes en la Escuela Nacional de Estudios Profesionales Aragón donde el alumno lleve a cabo prácticas que le auxiliaran en su formación profesional y de este modo poseerá el perfil profesional que las empresas requieren para cubrir sus necesidades.

Esta demanda de personal calificado ha llegado a modificar los planes de estudio de algunas carreras universitarias, de hecho algunas nuevas profesiones referentes al cómputo y a las telecomunicaciones han aparecido. Para aquellos que ya cumplieron con una etapa educativa universitaria, los nuevos retos exigen una actualización constante para no quedar rezagados. Tan solo los materiales educativos como los libros presentan importantes cambios en cada edición y aparecen nuevos temas que se desconocían hasta hace algunos años. Es común encontrar cursos de capacitación en las empresas para sus empleados con la intención de que puedan estar al día en materia de computación y telecomunicaciones. Es muy importante para cualquier organización o persona que la información que vaya a ser manejada a través de una red de datos sea confiable y segura de esta manera es poco conveniente que estas actividades las realicen personal con insuficiente capacidad.

La Universidad Nacional Autónoma de México es en cada ciclo escolar una de las escuelas a nivel medio y superior más demandadas por la población estudiantil mexicana, se encuentra involucrada junto con otras instituciones en varios proyectos de desarrollo tecnológico, cuenta con equipo de vanguardia para mantener su red académica, y entre sus opciones de carreras referentes al cómputo se encuentra la Ingeniería en Computación impartida en Ciudad Universitaria y ENEP Aragón. Refiriéndonos a este último plantel se tiene en el plan de estudios de ésta carrera la asignatura de Redes de computadoras impartida en el décimo semestre, en esta asignatura el profesor instruye la parte teórica pero se deja de lado una de las partes más importantes que es la práctica donde el alumno tiene contacto real con las aplicaciones de las de computadoras.

Por esta razón este trabajo de tesis propone la implantación de un laboratorio de redes de computadoras para esa asignatura incluida en el plan de estudios de la carrera de Ingeniería en Computación en la Escuela Nacional de Estudios Profesionales plantel Aragón con el fin de mejorar el nivel educativo del alumno. La propuesta del laboratorio plante de la siguiente manera:

En el capitulo uno de este trabajo se presenta todo un marco teórico de los protocolos TCP/IP ya que las prácticas que se proponen en este trabajo corresponde a la parte de la asignatura donde se les instruye a los alumnos el tema de protocolos.

El capitulo dos habla del perfil actual que los egresados de carreras tiene como común denominador este tema deben poseer, sus conocimientos de redes de computadoras, se hace una comparación con diferentes Universidades de México y sus métodos de enseñanza de la asignatura de redes y los mas importantes, el análisis de conocimientos y capacidades que demuestran alumnos que tomaron esta materia brindándoles un conocimiento práctico al darles la posibilidad de cursar un laboratorio de redes.

Basándonos en el modelo de La Asociación Nacional de Instituciones de Educación en Informática (ANIEI), el cual señala los conocimientos y funciones que determinan con precisión que conocimientos debe saber un profesional de la computación, se analizaron y compararon los perfiles que ofrecen las principales universidades, consideradas importantes por el número de matricula que presentan, dando como resultado un análisis en porcentaje de conocimientos adquiridos por el alumno.

La propuesta de mejorar el nivel de aprendizaje en las redes de computadoras para los alumnos de Ingeniería en Computación de la Escuela Nacional de Estudios Profesionales plantel Aragón se verá en el capitulo 3, se presenta un plan de prácticas propuestas a realizar dentro del tema Protocolos TCP/IP de la signatura de Redes de Computadoras, se describe a detalle las necesidades que deberán cubrirse por parte de la escuela y de los alumnos.

Por último se presentan las conclusiones de esta propuesta del Laboratorio de Redes.

Capítulo 1

Protocolo TCP/IP

1.1 GENERALIDADES

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos por la ISO, IICC, etc.

Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU), y con la expansión de la INTERNET se ha convertido en una de las arquitecturas de redes más difundida.

1.1.1 Historia

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPAnet) que conectaba redes de ordenadores de varias universidades y laboratorios de investigación en Estados Unidos. El servicio de navegación World Wide Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés).

El protocolo original se conocía como NCP "Network Control Protocol", el cual fue cambiado por un nuevo estándar más sofisticado, llamado TCP/IP, publicado en año de 1973 por Vint Cerf y Bob Kahn. TCP (Transmission Control Protocol) convierte mensajes en cadenas de paquetes en el nodo de origen, y los ensambla de nuevo en el punto de destino. IP (Internet Protocol) maneja el direccionamiento permitiendo que los paquetes fueran ruteados a través de diferentes nodos y hasta de diferentes redes.

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la

Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa.

En 1977, comenzó a extenderse el uso de TCP/IP en otras redes para vincularse a ARPANET.

A finales de los años 70 y los 80, personas de diferentes grupos sociales tuvieron acceso a computadoras de gran capacidad, siendo bastante fácil el conectarse a la creciente red de redes. Fue en esta época donde surgió USENET, el boletín electrónico más grande del mundo, basándose en UUCP, tecnología desarrollada en los laboratorios Bell de AT&T, junto con el sistema operativo UNIX, que al paso de los años, se ha convertido en el sistema operativo estándar de todas las computadoras conectadas.

En 1982, el Departamento de Defensa de los Estados Unidos declara como estándar al conjunto TCP/IP, separándose de ARPANET la parte militar, MILNET, dándose el auge por las estaciones de trabajo de escritorio, con sistema operativo Berkely UNIX (desarrollado por la Universidadde Berkeley, en California), que incluye software de red TCP/IP.

En 1983 se crea la EARN (European Academic and Research Network) para dar servicio a las universidades y centros de investigación europeos.

En 1984 Se instauran los servicios de denominación simbólica DNS (Domain Name Server).

World Wibe Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés), y en 1990 desaparece ARPANET

En 1992, las empresas y los medios de comunicación empiezan a interesarse por Internet. La Casa Blanca, la ONU y el Banco Mundial se conectan.

Durante 1993, la NSF (National Sciences Foundations) crea la Inter NIC para proveer servicios de información, así como registros, directorios y bases de datos referentes a Internet. En este momento los medios masivos de comunicación tradicional (radio, televisión y prensa escrita, entre otros) toman conciencia de Internet y sus implicaciones.

En 1994, Internet cumple sus 25 años de servicio. Y en 1995 Los sistemas de servicios vía modem comienzan a ofrecer servicios de Internet. Gran cantidad de compañías relacionadas a la red se vuelven públicas, encabezadas por Netscape, que tiene el tercer índice de ganancias jamás obtenido en aquel tiempo.

Hoy, en nuestros días, Internet y por ende, el uso de TCP/IP, se han convertido en un nuevo y revolucionario medio de comunicación a escala mundial.

1.1.2 Arquitectura de TCP/IP

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados a computadoras de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cuatro niveles o capas en las que se agrupan los protocolos (Figura 1), y que se relacionan con los niveles OSI de la siguiente manera:

- Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- Capa Inferior: TCP no define esta capa, pero dice que debe de haber algo que realice las funciones correspondientes a la capa de enlace y física del modelo OSI.

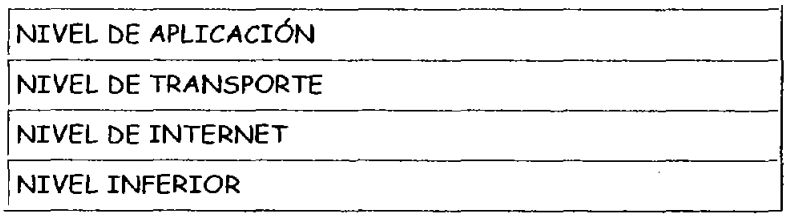


Figura 1. Arquitectura TCP/IP

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo

hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles (Figura 2).

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP cada una de estas unidades de información recibe el nombre de *"segmento"* y para IP se denomina *"datagrama"*, y son conjuntos de datos que se envían como mensajes independientes.

1.1.3 Protocolos TCP/IP

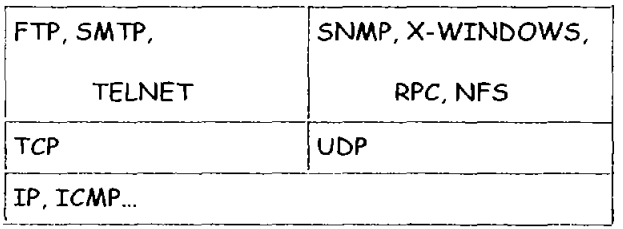


Figura 2. Familia de protocolos TCP/IP

- **FTP (File Transfer Protocol).** Se utiliza para transferencia de archivos.
- **SMTP (Simple Mail Transfer Protocol).** Es una aplicación para el correo electrónico.
- **TELNET:** Permite la conexión a una aplicación remota desde un proceso o terminal.
- **RPC (Remote Procedure Call).** Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- **SNMP (Simple Network Management Protocol).** Se trata de una aplicación para el control de la red.
- **NFS (Network File System).** Permite la utilización de archivos distribuidos por los programas de la red.
- **X-Windows.** Es un protocolo para el manejo de ventanas e interfaces de usuario.

1.1.4 Características del Protocolo TCP/IP

Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características.

- La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen *IP mueve los paquetes de datos a granel, mientras TCP se encarga del flujo y asegura que los datos estén correctos.*

- Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino. Compare esto con la manera en que se transmite una conversación telefónica. Una vez que establece una conexión, se reservan algunos circuitos para usted, que no puede emplear en otra llamada, aun si deja esperando a su interlocutor por veinte minutos.

- Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino. Éste, claro está, es el secreto de cómo se pueden enviar datos y mensajes entre dos computadoras aunque no estén conectadas directamente entre sí. Lo que realmente sorprende es que sólo se necesitan algunos segundos para enviar un archivo de buen tamaño de una máquina a otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples computadoras. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje.

- Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

- La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

Antes de continuar, veamos la relación de esta arquitectura con respecto al modelo de referencia OSI (Open Systems Interconnection) de la ISO.

Así como el modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por 4 niveles: el **nivel inferior** [enlace y físico], el **nivel de**

internet [ICMP, IP], **nivel de transporte** [TCP o UDP], y el **nivel de aplicación** [Telnet, FTP, SMTP].

1.1.5 El modelo OSI

El Modelo OSI fue desarrollado por la ISO (Organización Internacional de Estándares) con la intención de crear un estándar para los sistemas abiertos, es decir, para sistemas que trabajan con diferentes plataformas y deben estar abiertos a la comunicación con otros sistemas. El Modelo OSI se toma como un método universal de enseñanza y comprensión del funcionamiento de las redes. Este modelo consta de 7 capas (Figura 3 y 4), las primeras dos se encuentran implementadas en software y hardware, y las siguientes cinco solo en software.

Las capas del modelo OSI son las siguientes:

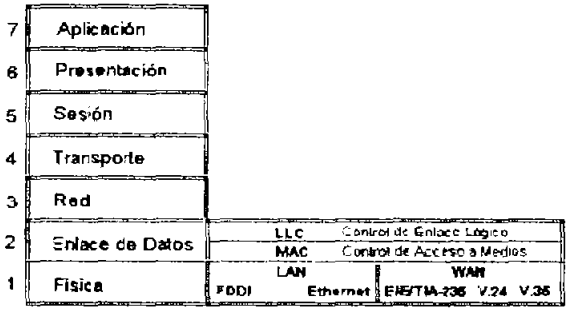


Figura 3.Capas del Modelo de Referencia OSI

- Capa **Física.** Se refiere a la transmisión de un flujo de bits a través de un canal de comunicación. En ésta se manejan los voltajes y pulsos eléctricos, además especifica cables y conectores. Dentro de esta capa se especifica el tipo de red: LAN o WAN, y en base a esto puede tomar diferentes tecnologías , ejemplo: para LAN, Ethernet, FDDI, Token ring, etc. y para WAN, EIA/TIA-232, V.24, V.35, etc.

- Capa **de Enlace de Datos.** Esta capa toma un transmisión de bits en bruto, lo transforma en una línea libre de errores en forma de tramas (las tramas son pequeños paquetes con datos que tienen una cabecera la cual, contiene la dirección de la máquina de inicio y la dirección de la máquina fina a quien se van a enviar los datos), transmite estas tramas, y si alguno falla, tiene la capacidad de retransmitirlo. La IEEE ha subdividido esta capa en dos partes: la subcapa LLC (Control de Enlace Lógico) que se encarga de administrar la comunicación entre dos dispositivos unidos en una red y soporta servicios orientados y no orientados a conexión; y la subcapa MAC (Control de Acceso a Medios) que administra el acceso al medio de transmisión físico de la red. Además existe una dirección MAC que es definida por la IEEE, la cual es una identificación única de cada dispositivo.

- **Capa de Red.** Cuando es necesario fragmenta la información de la capa de transporte en paquetes y los defragmenta al final. Su función principal es enrutar los paquetes es decir, establecer la ruta que deben seguir para llegar a su destino, además de verificar también que no se genere congestión en la red.

- **Capa de Transporte.** Establece las conexiones de red, puede crear una conexión distinta para cada conexión solicitada por la capa de sesión. Determina también que tipo de servicio proporcionará a la capa de sesión, puede ser: punto a punto sin errores o mensajes aislados sin garantía de entrega.

- **Capa de Sesión.** Permite a usuarios en diferentes máquinas establecer una conexión, en la que pueden transmitir datos. Controla el sentido del diálogo ya sea en un solo sentido o en ambos sentidos a la vez. Además tiene la función de sincronización para evitar que se retransmitan todos los datos en caso de una falla en la conexión, y así solo se transmitan los que faltan.

- **Capa de Presentación.** Establece una sintaxis y una semántica de la información transmitida, es decir, el formato. Define las estructuras de los datos a transmitir, compresión y criptografía.

- **Capa de Aplicación.** Aquí se encuentran los programas para transferencia de archivos, login remoto, correo electrónico, etc.

A continuación se puede observar una tabla donde se desglosan las capas del Modelo OSI y se muestran algunos protocolos utilizados en cada una de ellas (Figura 4).

MODELO OSI			
CAPA		**Protocolos Asociados**	**Dispositivos de conectividad**
7	APLICACIÓN	NFS X.400 X.500 Shell Redirector	
6	PRESENTACIÓN	SMB NCP NFS	
5	SESIÓN	TCP IPX	

		NetBIOS FTP/Telnet SMPT TFTP RPC SNMP	
4	TRANSPORTE	TCP UDP SPX/IPX	Gateway (Enrutador)
3	CAPA DE RED	IP IPX ICMP X.25	Enrutador
2B	ENLACE DE DATOS LLC	IEEE 802.2 ODI LABP NDIS Drivers	
2A	ENLACE DE DATOS MAC	IEEE 802.3 IEEE 802.5 CSMA/CD Token	Switch Puente (Bridge)
1	FÍSICA	IEEE 802.3 IEEE 802.4 IEEE 802.5 RS-232 RS-449 V.35 Topologías	Repetidor Transceptor MAU Hub NIC Cableado

Figura 4. Modelo OSI

1.2 CAPA DE RED

La capa de red se encarga de llevar paquetes de la fuente hasta su destino. Debe saber la topología de la subred de comunicaciones. Debe elegir una ruta adecuada para el envío de mensajes. Evita las rutas sobrecargadas y maneja situaciones dadas cuando la fuente y el destino se localizan en redes separadas.

1.2.1 Protocolo de Internet (IP)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más especifica como datagrama Internet o datagrama IP
Las características de este protocolo son:

- NO ORIENTADO A CONEXIÓN
- Transmisión en unidades denominadas **datagramas.**
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

La entrega del datagrama en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje. Por otra parte, el IP no contiene suma de verificación para el contenido de datos del datagrama, solamente para la información del encabezado.

En cuanto al ruteo (encaminamiento) este puede ser:

- Paso a paso a todos los nodos
- Mediante tablas de rutas estáticas o dinámicas

1.2.1.1 Direccionamiento IP

El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Únicamente el NIC (Centro de Información de Red) asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro) aparecen en la (Figura 5).

Clase	Rango decimal Del primer octeto	Bits de Orden Superior Del primer Octeto	ID de Red/host (R= red, H= host)	Máscara De subred predeterminada	Número de redes	Hosts Por red (direcciones utilizables)
A	1-126*	0	R.H.H.H	255.0.0.0	126 (2^7-2)	16.777.214 (2^{24}-2)
B	128-191	10	R.R.H.H	255.255.0.0	16.382 (2^{14}-2)	65.534 (2^{16}-2)
C	192-223	110	R.R.R.H	255.255.255.0	2.097.150 (2^{21}-2)	254 (2^8-2)
D	224-239	1110	Reservada par la multidifusión.			
E	240-247	11110	Experimental ;usada para investigación			

Figura 5. Clases de Direcciones

Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir. Local (hostid)) en donde se identifica la red y el host dentro de la red.

La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits (de orden más alto).

Las direcciones de las tres primeras clases sirven para la asignación de equipo.

Las direcciones de clase A sirven para redes de gran tamaño y su rango de direcciones varía desde la 0 la 127. La dirección 0 y la 127 están reservadas para propósitos ya definidos por lo tanto el rango útil va de la 1 a la 126.

Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde la 128 hasta la 191 .Esto permite tener 16320 redes con 65024 host en cada una.

Las direcciones de Clase C tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre la 192 y la 223, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Por último, las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde la 224 hasta la 239.

Cabe decir que, las direcciones de clase E comprenden el rango desde la 240 hasta la 247.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits. Por comodidad estos bits se representan como si estuviesen separados por un punto, por lo que el formato de dirección IP puede ser red.local.local.local para Clase A hasta red.red.red.local para clase C.

A partir de una dirección IP, una red puede determinar si los datos se enviarán a través de una compuerta (gateway, router). Obviamente, si la dirección de la red es la misma que la dirección actual (enrutamiento a un dispositivo de red local), llamado *host directo*), se evitará la compuerta; pero todas las demás direcciones de red se enrutarán a una compuerta para que salgan de la red local. La compuerta que reciba los datos que se transmitirán a otra red, tendrá entonces que determinar el enrutamiento con base en la dirección IP de los datos y una tabla interna que contiene la información de enrutamiento.

Otra de las ventajas que ofrece el direccionamiento IP es el uso de **direcciones de difusión** (*broadcast addresses*), que hacen referencia a todos los host de la misma red. Según la regla, cualquier dirección local (hostid) compuesta toda por 1s está reservada para difusión (broadcast). Por ejemplo, una dirección que contenga 32 1s se considera un mensaje difundido a todas las redes y a todos los dispositivos. Es posible difundir en todas las máquinas de una red alterando a 1s toda la dirección local o de anfitrión (hostid), de manera que la dirección 147.10.255.255 para una red de Clase B se recibiría en todos los dispositivos de dicha red; pero los datos no saldrían de dicha red.

Ejemplos prácticos:

EJEMPLO I

Consideremos la siguiente dirección IP en binario:

11001100.00001000.00000000.10101010 (204.8.0.170)

Según lo visto anteriormente, tenemos que la parte de la dirección 204.8.0 corresponde a una clase C y 170 corresponde a la dirección del equipo.

EJEMPLO II

Sea la dirección IP en binario:

10000100.11111000.10101101.00001111 (132.248.173.15)

Para este caso tenemos que la parte de de la dirección corresponde a 132.248, por lo que es una red de clase B, y la parte de la dirección que corresponde al equipo es 173.15.

EJEMPLO III

Sea la dirección IP en binario:

00001001.01000011.00100110.00000000 (9.67.38.0)

En este caso tenemos que la parte de la dirección corresponde a 9, por lo que es de clase A, y la dirección del equipo es 67.38.0.

1.2.1.2 Direcciones de red y de difusión

La mayor ventaja de la codificación de información de red en las direcciones de red en IP tiene una ventaja importante: hacer posible que exista un ruteo eficiente. Otra ventaja es que las direcciones de red IP se pueden referir tanto a redes como a anfitriones (hosts). Por regla, nunca se asigna un campo hostID igual a 0 a un anfitrión individual. En vez de eso, una dirección IP con campo hostID a 0 se utiliza para referirse a la red en sí misma. En resumen:

Las direcciones IP se pueden utilizar para referirse a redes así como a anfitriones individuales. Por regla, una dirección que tiene todos los bits del campo hostID a 0, se reserva para referirse a la red en si misma.

Otra ventaja significativa del esquema de direccionamiento IP es que éste incluye una dirección de difusión (BROADCAST) que se refiere a todos los anfitriones de la red. De acuerdo con el estándar, cualquier campo hostID consistente solamente en 1s, esta reservado para la difusión (BROADCAST). Esto permite que un sistema remoto envíe un sólo paquete que será difundido en la red especificada.

1.2.1.3 Resumen de reglas especiales de direccionamiento

En la práctica, el IP utiliza sólo unas cuantas combinaciones de ceros ("está") o unos ("toda"). Las posibilidades son las siguientes:

TODOS 0 - Éste anfitrión (permitido solamente en el arranque del sistema, pero nunca es una dirección válida de destino.

TODOS 0 | ANFITRIÓN - Anfitrión en ésta RED (solo para arranque, no como dirección. válida)

TODOS 1 - Difusión limitada (red local) (Nunca es una dirección válida de origen)

RED | TODOS 1 - Difusión dirigida para RED

127 | NADA (a menudo 1) - LOOPBACK (nunca debe aparecer en una red

Como se menciona arriba, la utilización de todos los ceros para la red sólo está permitida durante el procedimiento de iniciación de la maquina. Permite que una máquina se comunique temporalmente. Una vez que la máquina "aprende" su red y dirección IP correctas, no debe utilizar la red 0.

1.2.2 Protocolo de Resolución de Direcciones (ARP).

El objetivo es diseñar un software de bajo nivel que oculte las direcciones físicas (MAC) y permita que programas de un nivel más alto trabajen sólo con direcciones IP. La transformación de direcciones se tiene que realizar en cada fase a lo largo del camino, desde la fuente original hasta el destino final. En particular, surgen dos casos. Primero, en la última fase de entrega de un paquete, éste se debe enviar a través de

una red física hacia su destino final. La computadora que envía el paquete tiene que transformar la dirección IP de destino final en su dirección física (MAC). Segundo, en cualquier punto del camino, de la fuente al destino, que no sea la fase final, el paquete se debe enviar hacia un router intermedio. Por lo tanto, el transmisor tiene que transformar la dirección IP del router en una dirección física.

El problema de transformar direcciones de alto nivel en direcciones físicas se conoce como *problema de asociación de direcciones* (Address Resolution Problem). Este problema se suele resolver, normalmente, mediante tablas en cada máquina que contienen pares de direcciones, de alto nivel y físicas.

En el problema de asociación de direcciones en TCP/IP para redes con capacidad de difusión como Ethernet, se utiliza un protocolo de bajo nivel para asignar direcciones en forma dinámica y evitar así la utilización de una tabla de conversiones. Este protocolo es conocido como **Protocolo de Asociación de Direcciones (ARP** - *Address Resolution Protocol*). La idea detrás de la asociación dinámica con ARP es muy sencilla: cuando un host A quiere definir la dirección IP (IPb), transmite por difusión (broadcast) un paquete especial que pide al anfitrión (host) que posee la dirección IP (IPb), que responda con su dirección física (Pb). Todos los anfitriones reciben la solicitud, incluyendo a B, pero sólo B reconoce su propia dirección IP y envía una respuesta que contiene su dirección física.

Cuando A recibe la respuesta, utiliza la dirección física para enviar el paquete IP directamente a B. En resumen:

El ARP permite que un anfitrión encuentre la dirección física de otro anfitrión dentro de la misma red física con sólo proporcionar la dirección IP de su objetivo.

La información se guarda luego en una tabla ARP de orígenes y destinos.

I.2.3 Protocolo de Resolución de Direcciones Inverso (RARP)

Una máquina sin disco utiliza un protocolo TCP/IP para internet llamado RARP (Protocolo Inverso de Asociación de Direcciones) o Reverse Address Resolution Protocol, a fin de obtener su dirección IP desde un servidor.

En el arranque del sistema, una máquina de estas características (sin HDD permanente) debe contactar con un servidor para encontrar su dirección IP antes de que se pueda comunicar por medio del TCP/IP. El protocolo RARP utiliza el direccionamiento físico de red para obtener la dirección IP de la máquina. El mecanismo RARP proporciona la dirección hardware física de la máquina de destino para identificar de manera única el procesador y transmite por difusión la solicitud RARP. Los servidores en la red reciben el mensaje, buscan la transformación en una tabla (de manera presumible en su almacenamiento secundario) y responden al transmisor. Una vez que la máquina obtiene su dirección IP, la guarda en memoria y no vuelve a utilizar RARP hasta que se inicia de nuevo.

1.2.4 Protocolo de Mensajes de Control de Internet (ICMP).

Como hemos visto anteriormente, el Protocolo Internet (IP) proporciona un servicio de entrega de datagramas, no confiable y sin conexión, al hacer que cada router direccione datagramas. Si un router no puede, por ejemplo, rutear o entregar un datagrama, o si el router detecta una condición anormal que afecta su capacidad para direccionarlo (congestionamiento de la red), necesita informar a la fuente original para que evite o corrija el problema.

Para permitir que los routers de una red reporten los errores o proporcionen información sobre circunstancias inesperadas, se agregó a la familia TCP/IP un mecanismo de mensajes de propósito especial, el *Protocolo de Mensajes de Control Internet* (**ICMP**). El ICMP permite que los routers envíen mensajes de error o de control hacia otros routers o anfitriones, proporcionando una comunicación entre el software de IP en una máquina y el mismo software en otra.

Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

Formato de los mensajes ICMP

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo TYPE (TIPO) de mensaje, de 8 bits y números enteros, que identifica el mensaje; un campo CODE (CODIGO), de 8 bits, que proporciona más información sobre el tipo de mensaje, y una campo CHECKSUM (SUMA DE VERIFICACIÓN), de 16 bits. Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema.

La razón de regresar más que el encabezado del datagrama únicamente es para permitir que el receptor determine de manera más precisa qué protocolo(s) y qué programa de aplicación es responsable del datagrama.

El campo TYPE de ICMP define el significado del mensaje así como su formato. Los tipos incluyen (Tabla 1):

CAMPO TYPE	Tipo de Mensaje ICMP
0	Respuesta de ECO
3	Destino inaccesible
4	Disminución de origen (source quench) datagrama eliminado por congestión)
5	Redireccionar (cambiar una ruta)
8	Solicitud de ECO
11	Tiempo excedido para un datagrama
12	Problema de parámetros de datagrama
13	Solicitud de TIMESTAMP
14	Respuesta de TIMESTAMP
15	Solicitud de Información (Obsolete)
16	Respuesta de Información (obsoleto)
17	Solicitud de Máscara de dirección
18	Respuesta de máscara de dirección

Tabla 1. Campos Type de ICMP

Una de las herramientas de depuración más utilizadas incluye los mensajes ICMP de *echo request (8)* y *echo reply (0)*. En la mayoría de los sistemas, el comando que llama el usuario para enviar solicitudes de eco ICMP se conoce como **ping**.

1.3 CAPA DE TRANSPORTE

Provee comunicación de extremo a extremo desde un programa de aplicación a otro. Puede proveer un transporte confiable asegurándose de que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentran interactuando con la red simultáneamente de tal forma que los datos que envié una aplicación sean recibidos correctamente por la aplicación remota.

1.3.1 Protocolo de Control de Transmisión (TCP)

El TCP es el protocolo que se mencionó junto con el IP, el protocolo TCP toma la información que se desea enviar y la divide en segmentos, además, enumera cada segmento para que el receptor puede verificar la información y ponerla en el orden adecuado.

Para que el protocolo TCP pueda enviar esta secuencia de números a través de la red, cuenta con su propio mecanismo que le permite "escribir" en él la información requerida para su reordenamiento.

Del lado del destinatario, una parte del software del TCP reúne los paquetes, extrae la información de ellos y la pone en el orden adecuado, si algún paquete se pierde en la transmisión, el receptor solicita su retransmisión al emisor.

Una vez que el protocolo TCP tiene la información en el orden adecuado, la pasa a la aplicación del programa que este utilizando sus servicios.

1.3.1.1 Servicio de Transporte de Flujo Confiable

Ahora veremos el segundo servicio más importante y mejor conocido a nivel de red, la entrega de flujo confiable (Reliable Stream Transport), así como el Protocolo de Control de Transmisión (TCP) que lo define.

En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir debido a errores (falla el hardware, sobrecarga de la red,...). Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega de conexión y no confiable para transferencias de grandes volúmenes de información resulta ser la peor opción. Debido a esto, el TCP se ha vuelto un protocolo de propósito general para estos casos.

1.3.1.2 Unidades de datos del protocolo TCP

El TCP debe comunicarse con el IP en la capa de abajo (usando un método defino por el IP) y con las aplicaciones en la capa superior (usando los primitivos TCP-ULP). El TCP también debe comunicarse con otras implementaciones TCP a través de las redes. Para hacer esto, usa Unidades de Datos de Protocolo (Protocol Data Units, PDU), las cuales se llaman segmentos en el lenguaje TCP.

El diseño de las TCP (por lo común llamada encabezado) se muestran en la Figura 6.

<table>
<tr><td colspan="6">Puerto Fuente (16 bits)</td><td>Destino (16 bits)</td></tr>
<tr><td colspan="7">Número de Secuencia (32 bits)</td></tr>
<tr><td colspan="7">Número de acuse de recibo (32 bits)</td></tr>
<tr><td>Compensación de datos (4 bits)</td><td>Reservado (6 bits)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Ventana (16 bits)</td></tr>
<tr><td colspan="6">Suma de verificación (16 bits)</td><td>Señalador Urgente (16 bits)</td></tr>
<tr><td colspan="7">Opciones y Relleno</td></tr>
</table>

Figura 6. Encabezado TCP

Los diferentes campos son como siguen:

- *Puerto fuente*: Un campo de 16 bits que identifica al usuario TCP local (por lo general un programa de aplicación de capa superior).
- *Puerto Destino*: Un campo de 16 bits que identifica al usuario TCP de la máquina remota.
- *Número de Secuencia*: Un número que indica la posición del bloque actual en el mensaje total. Este número se usa también entre dos implementaciones TCP para proporcionar el número de secuencia de envío inicial (ISS).
- *Número de acuse de recibo*: Un número que indica el siguiente número de secuencia esperado. De una manera ambigua, éste muestra además el número de secuencia de los últimos datos recibidos; muestra el último número se secuencia recibido más 1.
- *Compensación de datos*: El número de palabras de 32 bits que están en el encabezado TCP. Este campo se usa para identificar el inicio del campo de datos.
- *Reservado*: Un campo de 6 bits reservado para uso futuro. Los bits 6 deben fijarse en 0.
- *Bandera Urg*: Si está activa (un valor de 1), indica que el campo del señalador urgente es significativo.
- *Bandera Ack*: Si esta activa, indica que el campo Acuse de recibo es significativo.
- *Bandera Psh*: Si esta activa, indica que la función push debe ejecutarse.
- *Bandera Syn*: Si está activa, indica que los números de secuencia deben sincronizarse. Esta bandera se usa cuando se está estableciendo una conexión.
- *Bandera Rst*: Si está activa, indica que la conexión debe reiniciarse.
- *Bandera Fin*: Si está activa, indica que el transmisor no tiene más datos que enviar. Éste es el equivalente de un marcador de fin de la transmisión.
- *Ventana*: Un número que indica cuántos bloques de datos puede aceptar la máquina receptora.
- *Suma de verificación*: Calculada tomando el complemento de uno de 16 bits, de la suma de complemento de uno de las palabras de 16 bits en el encabezado (incluyendo seudoencabezado) y texto juntos.
- *Señalador urgente*: Usado si se estableció la bandera urg; indica la parte del mensaje de datos que es urgente al especificar la compensación del número de secuencia en el encabezado. El TCP no toma ninguna acción específica con respecto a los datos urgentes, la acción la determina la aplicación.
- *Opciones*: Similar al campo Opciones del encabezado IP, éste se usa para especificar opciones del TCP. Cada opción consta de un número de opción (un byte), el número de bytes en ésta y los valores de la opción. En la actualidad, sólo están definidas tres opciones para el TCP:

  0 Fin de la lista de operaciones.
  1 No operación.
  2 Tamaño máximo del segmento.

- *Relleno*: Rellenado para asegurar que el encabezado es un múltiplo de 32 bits.

1.3.1.3 Puertos

Todas las aplicaciones de capa superior que usan el TCP tienen un número de puerto que identifica a la aplicación. En teoría, los números de puerto pueden asignarse en máquinas individuales o en cualquier parte que desee el administrador, pero se han adoptado algunas convenciones para permitir mejores comunicaciones entre las implementaciones TCP. Esto permite al número de puerto identificar el tipo de servicio que le está solicitando un sistema TCP a otro. Los números de puerto pueden cambiarse, aunque esto puede causar dificultades. La mayor parte de los sistemas mantienen un archivo de números de puerto y su correspondiente servicio.

De manera característica, los números de puerto arriba de 255 están reservados para su uso privado de la maquina local, pero los números por debajo de 255 se usan para procesos usados con frecuencia. Una lista de números de puerto usados con frecuencia la publica la Internet Assigned Numbers Authority /Autoridad de Números Asignados de Internet) y está disponible por medio de una RFC o, en muchos sitios que ofrecen archivos de resumen Internet para su transferencia. Por lo común, los números de puerto usados en esta lista se muestran en la Tabla 1. Los números 0 y 255 están reservados.

1.3.1.4 TCP y conexiones

El TCP tiene muchas reglas impuestas de la manera como comunica. Estas reglas y los procesos que sigue el TCP para establecer una conexión, transferir datos y terminar una conexión, por lo general se presentan en diagramas de estado. (Debido a que el TCP es un protocolo controlado por el estado, sus acciones dependen del estado de una bandera o creación parecida). Es difícil evitar los diagramas de estado demasiado complejos, de modo que pueden usarse diagramas de flujo como un método útil para entender al TCP.

Un punto extremo es un par de números enteros **(host, puerto)**, en donde *host* es la dirección IP de un anfitrión y *puerto* es el un puerto TCP en dicho anfitrión, esto es comúnmente conocido como *socket*.

Las conexiones vienen definidas por dos puntos extremos, y es más: la abstracción de la conexión para TCP permite que varias conexiones compartan un punto extremo (por ejemplo, varias conexiones en los mismos puertos). Esto es posible a que el TCP identifica una conexión por medio de un par de puntos extremos, y por eso varias conexiones en la misma máquina pueden compartir un número de puerto TCP.

El TCP combina la asignación dinámica y estática de puertos mediante un conjunto de *asignación de puertos bien conocidos* para programas llamados con frecuencia, pero la salida de la mayor parte de los números disponibles para el sistema se asigna conforme los programas lo necesitan.

La siguiente tabla muestra un ejemplo de números de puerto TCP asignados actualmente (Tabla 2).

DECIMAL	CLAVE	CLAVE UNIX	DESCRIPCIÓN
0			Reservado
1	TCPMUX		Multiplexor TCP
5	RJE		Introducción de unction remota
7	ECHO	echo	Eco
9	DISCARD	discard	Abandonar
11	USERS	systat	Usuarios activos
13	DAYTIME	daytime	Fecha, hora
15		netstat	Estado de red
17	QUOTE	qotd	Cita del día
19	CHARGEN	chargen	Generador de caracteres
20	FTP-DATA	ftp-data	Datos para FTP
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Conexión por terminal
25	SMTP	smtp	Protocolo de Transporte de Correo Sencillo
42	NAMESERVER	name	Nombre del host servidor
43	NICNAME	whois	Comando whois
53	DOMAIN	nameserver	Servidor de nombre de dominio (DNS)
79	FINGER	finger	Comando finger
93	DCP		Protocolo de Control de Dispositivo
101	HOSTNAME	hostnames	Servidor de Nombre de Anfitrión NIC
103	X400	x400	Servicio de correo X400
104	X400-SND	x400-snd	Envío de coreo X400

Tabla 2.Puertos TCP asignados actualmente.

1.3.1.5 Establecimiento de una conexión

Puede establecerse una conexión entre dos máquinas sólo si existe una conexión entre los dos sockets, ambas máquinas están de acuerdo en la conexión y ambas máquinas tienen recursos TCP adecuados, para servir a la conexión. Si no se cumple cualquiera de estas condiciones, no puede hacerse la conexión. La aceptación de conexiones la puede desencadenar una aplicación o una rutina de administración de sistema.

Cuando se establece una conexión se le dan ciertas propiedades que son válidas hasta que la conexión se cierra. De manera común, éstas son un valor de precedencia y un valor de seguridad. Estos parámetros los acuerdan las dos aplicaciones cuando la conexión está en el proceso de establecerse.

En la mayoría de los casos, una conexión la esperan dos aplicaciones, así que emiten solicitudes abiertas ya sea activas o pasivas. La Figura 7 muestra un diagrama de flujo para un TCP abierto. El proceso comienza con el TCP de la Maquina A, que recibe una solicitud para una conexión de su ULP, para lo cual envía un primitivo abierto activo a la Maquina B. El segmento que se crea tiene activada la bandera Syn y tiene asignado un número de secuencia. El diagrama muestra esto con la notación Syn SEQ 50, indicando que la bandera SYN está activada y que el número de secuencia (Initial Send Séquense, ISS) es 50. (Podría haberse elegido cualquier número).

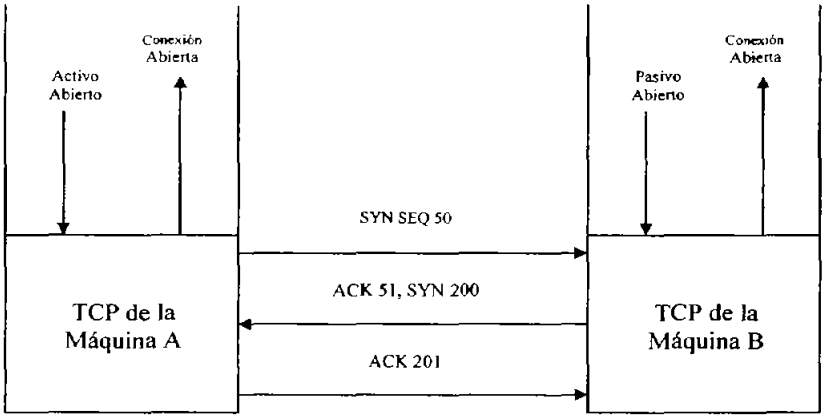


Figura 7. Establecimiento de una conexión

La aplicación en la Máquina B ha enviado una instrucción pasiva abierta a su TCP. Cuando se recibe el segmento SYN SEQ 50, el TCP de la Maquina 50, el TCP de la máquina B envía de regreso un acuse de recibo a la Máquina A, con el número de secuencia de 51. la Máquina B también establece por su cuenta un numero ISS. El diagrama muestra este mensaje como "ACK 51; SYN200", lo que indica que el mensaje es un acuse de recibo con el número de secuencia 51, tiene la bandera Syn activada y tiene u ISS de 200 (Figura 7).

Tras la recepción, la Máquina A envía de vuelta su propio mensaje de acuse de recibo con el número de secuencia establecido en 201. Esto es "ACK 201" en el diagrama. Luego, habiendo abierto y acusado recibo de la conexión, la Máquina A y la Máquina B envían mensajes de conexión abierta a través del ULP a las aplicaciones solicitantes.

No es necesario que la máquina remota tenga una instrucción pasiva abierta. En este caso, la máquina transmisora proporciona tanto el número de socket transmisor con el número de socket receptor, al igual que los valores de precedencia, seguridad y tiempo agotado. Es común que las dos aplicaciones soliciten un activo abierto al mismo tiempo. Esto se resuelve con bastante facilidad, aunque implica un poco más de tráfico en la red.

El servicio de transporte de datos TCP en realidad incluye las siguientes características:

- **Dúplex completo:** permite a ambos extremos de una conexión transmitir en cualquier momento, incluso de manera simultánea.
- **Oportunidad:** El uso de temporizadores asegura que los datos se transmitan dentro de un tiempo razonable.
- **Orden:** Los datos enviados desde una aplicación se reciben en el mismo orden en el otro extremo. Esto ocurre a pesar del hecho de que los datagramas podrían recibirse en desorden a través del IP, debido a que el TCP reensambla el mensaje en el orden correcto antes de pasarlo a las capas superiores.
- **Etiquetado:** Todas las conexiones han acordado un valor de precedencia y seguridad.
- **Flujo controlado:** El TCP puede regular el flujo de información utilizando búfer y límites de ventana.
- **Corrección de errores:** La suma de verificación asegura que los datos están libres de errores (dentro de los límites del algoritmo de la suma de verificación).

1.3.2 Protocolo de Datagrama de Usuario

La mayoría de los Sistemas Operativos actuales soportan multiprogramación. Puede parecer natural decir que un proceso es el destino final de un mensaje. Sin embargo, especificar que un proceso en particular en una máquina en particular es el destino final para un datagrama es un poco confuso. Primero, por que los procesos se crean y se destruyen dinámicamente, los transmisores rara vez saben lo suficiente para identificar un proceso en otra máquina. Segundo, nos gustaría poder reemplazar los procesos que reciben datagramas, sin tener que informar a todos los transmisores. Tercero, necesitamos identificar los destinos de las funciones que implantan sin conocer el proceso que implanta la función.

En vez de pensar en un proceso como destino final, imaginaremos que cada máquina contiene un grupo de puntos abstractos de destino, llamados ***puertos de protocolo***. Cada puerto de protocolo se identifica por medio de un número entero positivo.

Para comunicarse con un puerto externo, un transmisor necesita saber tanto la dirección IP de la máquina de destino como el número de puerto de protocolo del destino dentro de la máquina.

El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto en número de puerto de destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta.

El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. En resumen:

El UDP proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de la computadora anfitrión.

Formato de los mensajes UDP:

Cada mensaje UDP se conoce como *datagrama de usuario.* Conceptualmente, un datagrama de usuario consiste en dos partes: un encabezado UDP (Figura 8) y un área de datos UDP. El encabezado se divide en cuatro campos de 16 bits, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP.

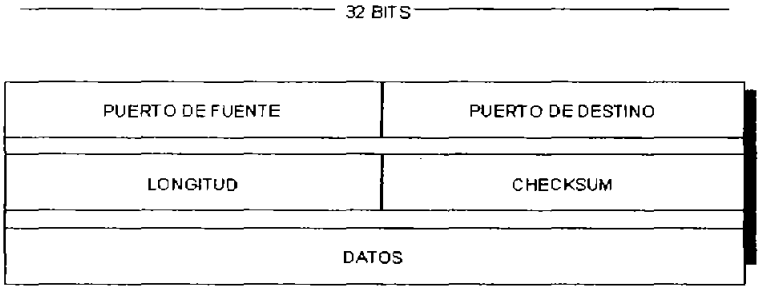


Figura 8. Encabezado UDP.

Los diferentes campos son como siguen:

- *Puerto fuente*: valor que identifica al puerto de proceso de aplicación remitente. Este campo es opcional en el caso de no ocuparse se coloca 0.
- *Puerto destino*: valor que identifica el proceso de recepción en la computadora destino.
- *Longitud*: valor que indica la longitud del datagrama de usuario, incluyendo la cabecera y los datos. La longitud mínima es de 8 octetos.
- *Checksum*: contiene el valor del complemento a 1 en 16 bits del complemento a 1 de la suma de seudocabecera de IP. se utiliza también en los campos de relleno.

1.4 CAPA DE APLICACIÓN

Esta capa corresponde a las aplicaciones que están disponibles para los usuarios, como TELNET, FTP, DNS, etc.

*1.4.1 Sistema de Nombre de Dominio (*DNS)

Los protocolos descritos anteriormente utilizan enteros de 32 bits, llamados direcciones de protocolo Internet (dirección IP) para identificar máquinas. Aún cuando cada dirección proporciona una representación compacta y conveniente para identificar la fuente y el destino en paquetes enviados a través de la red, los usuarios prefieren asignar a las máquinas nombres fáciles de recordar.

El DNS tiene dos aspectos conceptualmente independientes. El primero es abstracto. Especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto a los nombres. El segundo es concreto: especifica la implantación de un sistema de computación distribuido que transforma eficientemente los nombres en direcciones.

1.4.1.1 Resolución de nombres

Conceptualmente, la resolución de nombres de dominio procede de arriba hacia abajo, comenzando con el servidor de nombres raíz y siguiendo luego hacia los servidores localizados en las ramas del árbol de la red.

Hay dos formas de utilizar en sistema de nombres de dominio: contactar un servidor de nombres cada vez o solicitar al sistema de servidores de nombres que realice la traducción completa. En este caso, el software cliente forma una solicitud de nombres de dominio que contiene el nombre a resolver, una declaración sobre la clase del nombre, el tipo de respuesta deseada y un código que especifica si el servidor de nombres debe traducir el nombre completamente. Se envía la solicitud a un servidor de nombre para su resolución.

Cuando un servidor de nombres de dominio recibe una solicitud, verifica si el nombre señala un subdominio sobre el cual tenga autoridad. Si es así, traduce el nombre a una dirección de acuerdo con su base de datos y anexa una repuesta a la solicitud, antes de enviarla de regreso al cliente. Si el DNS no puede resolver el nombre completamente, verifica que tipo de interacción especificó el cliente. Si el cliente solicita una traducción completa (una *resolución recursiva* en la terminología DNS), el servidor se pone en contacto con un servidor de nombres de dominio que pueda resolver el problema del nombre y devuelve la respuesta al cliente.

Si el cliente solicita una resolución no recursiva (resolución iterativa), el servidor de nombres no puede dar una respuesta. Se genera una réplica que especifica el nombre del servidor que el cliente deberá contactar la próxima vez para resolver el nombre.

¿Cómo encuentra un cliente un DNS para comenzar la búsqueda?

¿Como encuentra un DNS a otros DNSs que puedan responder a las solicitudes que el no puede responder?

La respuesta es sencilla: Un cliente debe saber como contactar al último DNS para asegurarse de que el DNS puede alcanzar a otros, el sistema de dominio requiere que cada servidor conozca la dirección del último servidor en la raíz. Además, un servidor podría conocer la dirección de un servidor para el dominio de un nivel inmediatamente superior (llamado padre).

Los DNSs utilizan un puerto de protocolo bien conocido para toda comunicación, así, los clientes saben cómo comunicarse con un servidor una vez que conocen la dirección IP de la máquina que se conecta al servidor. No hay forma estándar que los anfitriones localicen una máquina en el entorno local, el cual corre un DNS; esto se encuentra abierto para quien diseñe el software cliente.

En algún sistema, la dirección de la máquina que proporciona el servicio de nombres de dominio está dentro de la frontera de los programas de aplicación en el tiempo de compilación, mientras que en otros la dirección se encuentra configurada dentro del S.O. en el arranque. En otros más, al administrador coloca la dirección de un servidor en un archivo en almacenamiento secundario (/etc/hosts).

1.4.2 Protocolo Telnet

El término Telnet se usa para referirse tanto al programa como al protocolo que proporciona estos servicios. El servicio Telnet se proporciona por medio del número de puerto 23 del TCP.

Pero, ¿Como definimos Telnet? Telnet es un protocolo de emulación de terminal normalmente usado en aplicaciones que usan línea de comando, en Internet.

Telnet se ideó debido a que en esa época el único método de que una máquina tuviera acceso a los recursos de otra máquina (incluyendo los discos duros y los programas almacenados ahí) era establecer un enlace, usando dispositivos de comunicaciones como módems o redes en puertos en serie dedicados o adaptadores de red. Esto es un poco más complicado de lo que podría parecer a primera vista, debido a la gran diversidad de terminales y computadoras, cada una con sus propios códigos de control y características de terminal. Cuando se conecta en forma directa con otra máquina, la CPU de la máquina debe manejar la traducción de los códigos de terminal entre las dos, lo cual carga a la CPU. Con varios registros remotos activos, la CPU de una máquina puede ocupar una cantidad desmesurada de tiempo manejando las traducciones. Esto es un problema, en especial con servidores que pueden manejar muchas conexiones a la vez: si cada una tuviera que manejarse con una traducción de terminal completa, la CPU servidora podría atascarse con sólo ejecutar esta función.

Telnet modera este problema incrustando las secuencias de las características de terminal dentro del protocolo Telnet. Cuando se comunican dos máquinas usando

Telnet, este puede determinar y establecer los parámetros de comunicaciones y de terminal para la sesión durante la fase de conexión. El protocolo Telnet incluye la capacidad de no soportar un servicio que no puede manejar un extremo de la conexión. Cuando una conexión se ha establecido por Telnet, ambos extremos han acordado un método para que las dos máquinas intercambien información, restándole carga a la CPU servidora de una gran cantidad de trabajo.

1.4.3 Protocolo FTP

El File Transfer Protocol, por lo general llamado FTP es un protocolo que permite transferir archivos entre dos máquinas conectadas a INTERNET, pudiendo con ello transferir al almacenamiento local de la máquina receptora, información de una máquina remota. Este Protocolo maneja archivos a través de máquinas sin tener que establecer una sesión remota con Telnet. El FTP permite transferir archivos en uno y otro sentido, administrar directorios y tener acceso al correo electrónico.

El FTP no está diseñado para permitir el acceso a otra máquina para ejecutar programas, pero es la mejor utilería para transferencias de archivos.

El FTP usa dos canales TCP. El puerto 20 del TCP es el canal de datos y el puerto 21 es el canal de comandos. El FTP difiere de la mayor parte de los demás programas de aplicación TCP/IP donde usa dos canales, permitiendo la transferencia simultanea de comandos FTP y datos. También difiere en otro aspecto importante: el FTP realiza todas las transferencias de archivo en primer plano, en lugar de hacerlo en el segundo plano. En otras palabras, el FTP no usa colas, de modo que se observa el proceso de transferencia en tiempo real.

Al usar el TCP, el FTP elimina la necesidad de preocuparse por la confiabilidad o la administración de la conexión, debido a que el FTP puede basarse en el TCP para ejecutar estas funciones en forma apropiada.

En lenguaje del FTP, los dos canales que existen entre las dos máquinas se llaman Protocol Interpreter (interprete del protocolo), o PI, y Data Transfer Process (proceso de transferencia de datos), o DTP. El PI transfiere instrucciones entre las dos aplicaciones usando el canal 21 de comandos TCP y el DTP transfiere datos en el canal 20 de datos TCP.

1.5 IPV6

Cuando se creó el IP versión 4 (la versión actual), el uso de una dirección IP de 32 bits parecía más que suficiente para manejar el uso proyectado de Internet. Sin embargo, con el índice de crecimiento increíble de Internet durante los últimos años, la dirección IP de 32 bits podría volverse un problema. Para contrarrestar este límite, el IP Next Generation (IP Siguiente Generación), por lo general llamado IP versión 6 (Ipv6), está en elaboración.

En la actualidad, se están estudiando varias propuestas para la realización del Ipng, la mas popular de las cuales son TUBA (TCP y UDP con direcciones más grandes) , CATNIP (Arquitectura Común para Internet) y SIPP (Protocolo Internet Simple Plus). Ninguna de las tres satisface todos los cambios propuestos para la versión 6, pero es probable un compromiso o modificación basados en una de estas propuestas.

¿Qué tiene que ofrecer el IPng? La lista de cambios indica las principales características de IPng en forma abreviada:

- Dirección de red de 128 bits en lugar de 32 bits.
- Encabezado IP más eficiente con extensiones para aplicaciones y opciones.
- Sin suma de verificación de encabezado.
- Una etiqueta de flujo para requerimientos de calidad del servicio.
- Prevención de fragmentación intermedia de datagramas.
- Seguridad incorporada para autentificación y encriptación.

A continuación se verá el IPng con un poco más de detalle para mostrar los cambios que afectan a la mayoría de los usuarios, así como a los programadores de red y administradores de red. Comenzaremos con un vistazo al encabezado IPng. Recuerde que en la actualidad el IPng todavía esta en elaboración y no está desplegado en forma amplia. Con excepción de redes de prueba.

Datagrama IPng

Como se mencionó antes, el encabezado para los datagramas Ipgn se ha modificado a partir del encabezado de la versión 4 anterior. Los cambios son principalmente para proporcionar soporte a las nuevas direcciones IP más largas de 128 bits y para eliminar los campos obsoletos e innecesarios. El diseño básico del encabezado IPng se muestra en la Figura 1. Como se puede ver, hay bastantes cambios con respecto al encabezado IP usado en el IP versión 4.

El número de versión en el encabezado del datagrama IP es de 4 bits de largo y contiene el número de versión (el cual es 6 en el IPng). El campo prioridad tiene 4 bits de largo y contiene un valor que indica la prioridad del datagrama. Ésta se usa para definir el orden de transmisión. La prioridad se establece primero con una clasificación amplia y, luego, un identificador más reducido dentro de cada clase.

El campo Etiqueta de flujo tiene 24 bits de largo y todavía está en la capa de elaboración. Es probable que se use en combinación con la dirección IP de la máquina fuente para proporcionar identificación de flujo para la red. Por ejemplo, si se está usando una estación de trabajo UNÍS en la red, el flujo es diferente de otra máquina como una PC Windows XP. Este campo se puede usar para identificar características del flujo y proporcionar algunas capacidades de ajuste. El campo también se puede usar para ayudar a identificar las máquinas de destino para transferencias grandes, en cuyo caso u sistema caché se vuelve más eficiente al enrutar entre la fuente y el destino.

El campo Longitud de carga útil es un campo de 16 bits usado para especificar la longitud total del datagrama IP, dada en bytes. La longitud total es exclusiva del encabezado IP en sí. El uso de un campo de 16 bits limita el valor máximo en este campo a 65,535, pero hay una provisión para enviar datagramas grandes usando un encabezado de extensión.

El campo Encabezado siguiente se usa para indicar cuál sigue al encabezado IP cuando otras aplicaciones desean viajar a cuestas en el encabezado IP. Se han definido diversos valores para el campo Encabezado siguiente. Figura
El campo límite de salto determina el número de saltos que puede viajar el datagrama. Con cada avance, el número disminuye en 1. Cuando el campo límite de salto alcanza el 0, el datagrama se desecha, igual que en el IP versión 4.

Por último, se colocan en el encabezado de las Direcciones IP Transmisora y Destino con formato de 128 bits.

Direcciones IP de 128 bits

Con toda probabilidad el aspecto más importante del IPng es su capacidad para proporcionar direcciones IP más largas. IPng aumenta la dirección IP de 32 bits a 128 bits. Esto permite que ensamble una cantidad increíble de direcciones, probablemente más de las que pueden usarse.

Las direcciones IP nuevas soportan tres clases de direcciones: unicast (emisión única), multicast (emisión multiple) y anycast (cualquier emisión).

- Las direcciones unicast tienen la intención de identificar la interfaz de una máquina particular. Esto permite a una PC, por ejemplo, tener en uso varios protocolos diferentes, cada uno con su propia dirección. Por tanto, se podrían enviar mensajes de manera específica a la dirección de interfaz IP de una máquina y no a la dirección de interfaz NetBEUI.
- Una dirección multicast identifica un grupo de interfaces, permitiendo a todas las máquinas en un grupo recibir el mismo paquete. Esto es muy parecido a las emisiones en el IP versión 4, aunque con más flexibilidad para definir grupos. Las interfaces de su máquina podrían pertenecer a varios grupos multicast.
- Una dirección anycast identifica a un grupo de interfaces en una dirección multicast única. En otras palabras, el datagrama puede recibir más de una interfaz en la misma máquina.

El manejo de la fragmentación y el reensamblaje también se cambia con el IPng para proporcionar más capacidades para el IP. También está un esquema de autentificación propuesto por el IPng, que puede asegurar que los datos no se han dañado entre el transmisor y el receptor, así como asegurar que las máquinas transmisora y receptora son quienes dicen ser.

Encabezados de extensión IP

IPng tiene la disposición de permitir que se añadan encabezados adicionales al encabezado IP. Esto puede ser necesario cuando no es posible un enrutamiento sencillo hacia el destino o cuando se requieren servicios especiales para el datagrama, como una autentificación. La información adicional requerida se empaca en un encabezado de extensión y anexa al encabezado IP.

IPng define varios tipos de encabezados de extensión identificados por un número colocado en el campo Encabezado siguiente del encabezado IP y se listan a continuación.

- Encabezados salto a salto.
- Encabezados de enrutamiento.
- Encabezados de fragmentación
- Encabezados de autentificación.

Con esto concluimos el capitulo referente a los protocolos TCP/IP, en el que se muestra el nacimiento, evolución, caracteristicas y tareas mas notables de los principales protocolos de este amplio conjunto, el cual es utilizado por los equipos conectados a Internet, para obtener y mantener comunicación entre sí.

Damos paso al Capítulo 2 "Análisis de la materia de Redes de computadoras", en el cual, hablaremos de la importancia que tienen los laboratorios para ampliar, desarrollar y comprobar los conocimientos expuestos en teoría, así como la necesidad de impartir un Laboratorio de Redes en la E.N.E.P. Aragón, como también los métodos de enseñanza que tienen algunas de las mas reconocidas Universidades en México para impartir esta materia tan primordial, refiriéndose a los conocimientos básicos y necesarios que todo Ingeniero en Computación debe tener respecto a las Redes de Computadoras.

Capítulo 2

Análisis de la materia de Redes de Computadoras.

Una de las misiones de la ENEP Aragón dentro de la carrera de Ingeniería en Computación es mejorar continuamente la calidad de la educación que brinda a sus estudiantes; de forma tal que ésta permita desarrollar en ellos habilidades para evaluar argumentos, analizar situaciones particulares del mundo real y pensar como Ingenieros, pero que, además, satisfaga tanto sus necesidades individuales como sociales. Por lo tanto, los sujetos directamente involucrados en el proceso de enseñanza-aprendizaje, es decir, profesores y estudiantes, son los llamados a desarrollar una metodología de enseñanza que logre cumplir con esos objetivos.

Es importante señalar que para poder cumplir con esos objetivos, y siendo más específicos, dentro de la materia de Redes se trata de lograr la implementación de un laboratorio de Redes a través del cuál los alumnos apliquen sus conocimientos teóricos.

Este capítulo pretende, por consiguiente, identificar los métodos de enseñanza más utilizados por los profesores de la materia de Redes de algunas Universidades lo cual nos dará una indagación preliminar del estado actual de la metodología empleada para enseñar la materia de Redes.

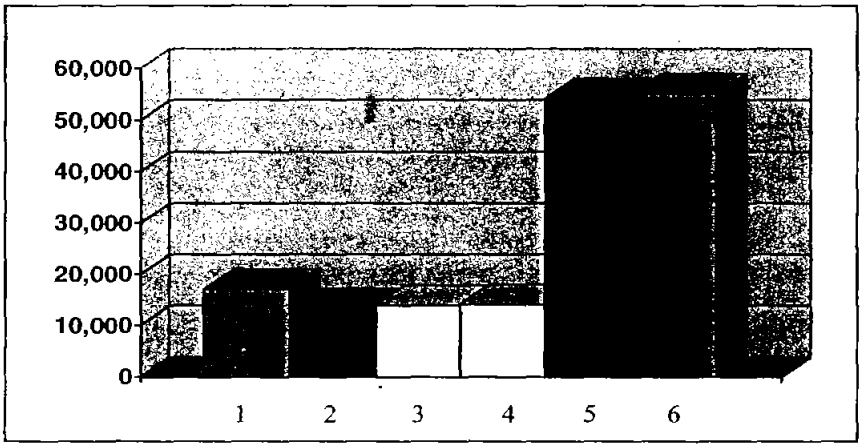
2.1. DEMANDA DE UNIVERSIDADES PARA CARRERAS A FINES A LA COMPUTACIÓN

Las últimas estadísticas para el periodo 2000-2001 de la Secretaria de Educación Publica nos indica que existen poco más de dos millones de personas en la Republica Mexicana inscritas en alguna carrera técnica superior, licenciatura o posgrado. La Universidad Nacional Autónoma de México tiene una matricula de 105,509 alumnos registrados en educación superior a nivel general solo en el Distrito Federal, ocupando el primer lugar de población estudiantil, y el Instituto Politécnico Nacional con una matricula de 75,214 ocupa el segundo lugar.

De acuerdo con el Instituto Nacional de Estadística Geográfica e Informática (INEGI), la matrícula de carreras de licenciatura vinculadas con tecnología de información, ha tenido un crecimiento sostenido y constante, alcanzando a duplicarse en los últimos 10 años.

De los 167,711 alumnos hasta el año 2001, 5 de las 35 carreras que se ofrecen abarcan el 89.8% del universo reseñado. Estas carreras son Informática, Ingeniero en Sistemas Computacionales, Informática Administrativa, Computación e Ingeniería en Computación. La distribución de matrícula para estas carreras se puede ver en la siguiente Gráfica 1.

1- Otras 30	17,069
2- Ing. Computación	13,367
3- Computación	13,888
4- Informática Administrativa	14,104
5- Ing. Sistemas Computacionales	54,151
6- Informática	55,132



Gráfica 1.Educación en Computación e Informática en México.
Licenciaturas e Ingenierías con mayor matrícula en 2000-2001.

En las 32 entidades de la República Mexicana existen programas de estudio a nivel licenciatura relacionados con la informática y la computación. El Distrito Federal tiene el índice más alto de concentración de matrícula de las carreras de Licenciatura en Computación y Sistemas con un 14.3% a nivel nacional, el Estado de México ocupa el segundo lugar con un 9.5%. Estos porcentajes se muestran a continuación en la Tabla 1.

ENTIDAD	PORCENTAJE	ENTIDAD	PORCENTAJE
Aguascalientes	1.0%	Nayarit	0.8%
Baja California	2.9%	Nuevo León	4.4%
Baja California Sur	0.5%	Oaxaca	2.2%
Campeche	0.9%	Puebla	4.7%
Chiapas	2.6%	Querétaro	1.4%
Chihuahua	3.2%	Quintana Roo	0.5%
Coahuila	3.3%	San Luis Potosí	1.9%
Colima	0.8%	Sinaloa	2.9%
Distrito Federal	14.3%	Sonora	2.6%
Durango	1.4%	Tabasco	3.3%
Guanajuato	3.1%	Tamaulipas	6.3%
Guerrero	2.6%	Tlaxcala	0.8%
Hidalgo	1.5%	Veracruz	8.0%
Jalisco	5.7%	Yucatán	1.5%
México	9.5%	Zacatecas	1.1%
Michoacán	2.4%		
Morelos	1.8%	**TOTAL**	**100%**

Tabla 1. Indice de concentración de matrículas de las carreras
De licenciatura en Computación y Sistemas año 2001 Fuente INEGI.

Las principales escuelas en donde se imparten carreras relacionadas con el cómputo son la Universidad Nacional Autónoma de México, Universidad Autónoma Metropolitana, Instituto Politécnico Nacional y el Instituto Tecnológico de Estudios Superiores Monterrey campus Ciudad de México de acuerdo a la matrícula que estas instituciones presentaron en el año 2000.

A continuación se presentan las estadísticas de estas cuatro instituciones referentes a la carrera que imparten relacionada con el cómputo. Estas estadísticas corresponden al año 2003 Tabla 2.

Institución	Primer Ingreso			Primer Ingreso y Reingreso			Egresados 2003			Titulados 2003		
	H	M	Total	H	M	Total	H	M	Total	H	M	Total
Universidad Nacional Autónoma de México	14502	15557	30059	63817	67674	131491	12060	14675	26735	5888	7013	12901
Instituto Tecnológico de Estudios Superiores Monterrey	5806	4036	9842	31054	21584	52638	3791	2850	6641	3765	2717	6552
Universidad del valle de México	3672	3958	7630	13918	15954	29872	890	1086	1976	955	1233	2188
Instituto Politécnico Nacional	10564	8323	18887	44554	33411	77965	7581	6055	13636	5625	4342	9967

Tabla 2 Matrículas de las carreras relacionadas con el cómputo y las comunicaciones
Impartidas en las principales Instituciones Educativas en el Distrito Federal.
Año 2003 Fuente ANUEIS

Sigue siendo la UNAM la institución que más alumnos atiende en los aspectos de reingreso. Alumnos titulados y egresados. Para complementar esta tabla solo agregaremos la matrícula de la Escuela Nacional de Estudios Profesionales plantel Aragón en la carrera de Ingeniería en Computación y son los datos que se presentan a continuación en la Tabla 3.

Escuela y Carrera	1er Ingreso	1er Ingreso y Reingreso	Egresados 2003	Titulados 2003
Universidad Nacional Autónoma de México Escuela Nacional de Estudios Profesionales Plantel Aragón, Ingeniería en Computación.	258	1368	137	90

Tabla 3. Matrícula de la carrera de Ingeniería en computación impartida en la E.N.E.P. plantel Aragón. Año 2003 Fuente ANUIES

La matricula de la E.N.E.P. Aragón solo está por debajo de la registrada por la Facultad de Ingeniería de la propia UNAM formando así , parte de las principales escuelas, por matrícula, que ofrecen un programa educativo referente al cómputo.

En lo que se refiere a posgrado en 8 de 32 entidades no se imparte algún programa educativo de maestría, estas entidades son: Chiapas, Michoacán, Durango, Nayarit, Quintana Roo, Tabasco, Yucatán y Zacatecas. El 28% de las entidades del país (9) registran instituciones que ofrecen programas de doctorado, a continuación se muestran estas entidades con su respectivo programa e institución en la Tabla 4.

Entidad	Institución	Programa
Baja California	Centro de Investigación Científica y Educación Superior de Ensenada	Computación
Distrito federal	IPN, UAM, UNAM	Computación e Ingeniería en Computación
Estado de México	Instituto Tecnológico de Toluca	Computación
Morelos	ITESM	Computación
Nuevo León	ITESM	Informática
Oaxaca	Universidad Tecnológica de la Mixteca	Computación
Puebla	Instituto Nacional de Astrofísica Óptica y Electrónica	Ingeniería Computacional
Sinaloa	Universidad Autónoma de Sinaloa	Computación
Veracruz	Instituto de Ecología	Sistemática

Tabla 4. Educación en Computación e Informática en México, año 2003
Cobertura: Doctorado, Fuente: DGES.

De acuerdo a las estadísticas la educación en computación e informática en México ha incrementado su demanda principalmente en el nivel de licenciatura y se muestra en la siguiente Tabla 5.

Área Subarea Concentración	Primer Ingreso			Primer Ingreso y Reingreso			Egresados 2003			Titulados 2003		
	H	M	Total	H	M	Total	H	M	Total	H	M	Total
Ing. en Cibernética y Electrónica	37	9	46	136	22	158	17	4	21	6	1	7
Ing. en Cibernética y Sistemas Computacionales	226	44	270	750	165	915	106	20	126	120	40	160
Ing. en Ciencias Computacionales	3289	1130	4419	11859	4414	16273	1036	474	1510	503	233	736
Ing. en Computación y Sistemas Digitales	77	31	108	254	161	415	31	18	49	18	3	21
Ing. en Comunicación Multimedia	55	101	156	219	155	374						
Ing. en Desarrollo Computacional	2		2	104	43	147	12	8	21	4		4
Ing. en Informática	409	249	658	1441	787	2228	31	21	52	9	11	20
Ing. en Sistemas	362	117	479	1026	309	1335	67	23	90	27	16	43
Ing. en sistemas Computacionales	13389	5661	19050	47892	20785	68677	3888	2047	5935	2259	1252	3511
Ing. en Sistemas de Información	327	98	425	1097	352	1449	124	57	181	87	32	119
Ing. en Sistemas y Comunicaciones	129	33	162	631	190	821	31	23	54	7	5	12
Lic. en Ciencias Computacionales	1323	489	1812	4559	2166	6725	417	354	771	274	178	452
Lic. en Informática	10587	8796	19383	40184	35288	75472	5391	5086	10477	2412	2736	5148
Lic. en sistemas Computacionales	1686	858	2544	6225	3488	9713	628	433	1061	377	228	605
Lic. en Sistemas de Computación Administrativa	1400	1192	2592	5472	4291	9763	609	586	1195	287	284	571
Lic. en Sistemas de Información Administrativa	136	109	245	863	760	1623	94	180	174	71	39	110

Tabla 5. Matrículas de las carreras relacionadas con el cómputo y las comunicaciones.

Algunas empresas integradoras, se han involucrado en la educación ofreciendo servicios de capacitación en el área de redes otorgando certificados, algunas instituciones educativas realizan acuerdos con estas empresas para incluir programas de certificación en sus planes de estudio.

Entre los servicios más ofrecidos en los últimos años por las principales empresas integradoras, como son Cisco, IBM, Microsoft, 3Com y Novell, se encuentran el diseño e implantación de las redes locales corporativas, la administración de redes y las telecomunicaciones. Recordemos que estas tareas forman parte de una de las áreas de estudio que se incluye en las carreras relacionadas con la informática y la computación, el área de redes.

En los últimos años han surgido organismos no gubernamentales que han llevado la acreditación de programas educativos, el Consejo de Acreditación de la Enseñanza de la Ingeniería (CACEI) y el Consejo Nacional de Acreditación en Informática y Computación (CONAIC) son algunos de ellos.

A continuación veremos la forma en que son aplicados los métodos de estudio de algunas universidades en México.

2.2 MÉTODOS DE ENSEÑANZA EN ALGUNAS UNIVERSIDADES DE MÉXICO.

Para llegar al nivel de desarrollo independiente en Informática y Computación que el país requiere es de suma importancia formar profesionales sólidamente preparados. El área de redes tratada en cada uno de los planes de estudio puede variar según el perfil de la profesión. La Asociación Nacional de Instituciones de Educación en Informática (ANIEI) estableció un comité de Modelos curriculares en dónde se señalan los conocimientos y funciones que determinen con precisión que debe saber y hacer un profesional de la computación.

La ANIEI se fundó en la ciudad de Guadalajara el 8 de Octubre de 1982 y su esencia y espíritu están dados por el objetivo de contribuir a la formación de profesionales en Informática y Computación sólidamente preparados, a demás de impulsar la difusión y la asimilación de una cultura computacional en la sociedad.

La ANIEI está integrada por asociados y miembros. Los asociados son instituciones educativas de nivel medio superior y postgrado que tengan programas de formación en Informática y Computación y que estén organizados con base en los ordenamientos estatales sobre educación. Se consideran como miembros a todos aquellos institutos, facultades, escuelas, centros, colegios y campus que pertenezcan a los asociados, quienes están representados por su máxima autoridad o su delegado. Algunas de estas Instituciones son las siguientes:

- Universidad Autónoma Metropolitana.
- Benemérita Universidad Autónoma de Puebla.
- Universidad Autónoma de Nuevo León.
- Colegio Nacional de Educación Profesional Técnica.
- Instituto Tecnológico de Estudios Superiores Monterrey Campus Monterrey.
- Universidad Autónoma de Querétaro.
- Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas (UPPICSA) – Instituto Politécnico Nacional.
- Dirección general de Servicios de Cómputo Académico (DGESCA) – Universidad Nacional Autónoma de México.

Entre los principales objetivos del ANIEI están los siguientes:

i. Propugnar para que las instituciones de educación en informática del país prepare profesionistas con sentido de servicio a la comunidad, capaces de actuar como agentes de cambio para el desarrollo del país.
ii. Contribuir a la integración, actualización y superación de la educación en informática, en todos sus niveles.
iii. En materia de docencia. Analizar los problemas relacionados con la enseñanza de la informática, proponer soluciones y colaborar en su implantación.

La ausencia en la definición de un núcleo básico de conocimientos y funciones que determinen con precisión qué debe saber y qué hacer un profesional de la computación o de la informática originó que la ANIEI formará el comité de modelos curriculares. El comité presentó la primera versión de los modelos curriculares en 1984, que muestran el perfil de un profesional en el cómputo y la informática. Estos modelos han sufrido cambios en el transcurso de los años, los datos que aquí se mencionan forman parte de la última revisión hecha en el año 2000.

Uno de los perfiles que la ANIEI define es el de Ingeniero en Computación, aquí al igual que para otros tres perfiles se definen ocho grandes áreas de estudio, una de ellas la de redes. Tomando porcentajes de cada una de las áreas de estudio, la ANIEI propone un 12.5% de conocimientos en redes para Ingeniería en Computación.

El ANIEI sugiere para cubrir el área de redes 5 principales temas, que son los siguientes:

- ✓ Transmisión y comunicación de datos.
- ✓ Topologías.
- ✓ Protocolos para comunicación.
- ✓ Intercomunicación de redes.
- ✓ Seguridad e Integridad de la Información.

Comparemos ahora la propuesta del ANIEI con algunas carreras de Ingeniería referentes a la computación. Se tomaron aquellos planes de estudio que se semejan más con la carera de Ingeniería en Computación y/o que a demás forman parte de las principales instituciones educativas que por su matricula destacan de entre las demás.

A) Universidad Nacional Autónoma de México, Escuela Nacional de Estudios Profesionales, Plantel Aragón.
Ingeniería en Computación

La carrera de Ingeniería en Computación en la UNAM es impartida en Ciudad Universitaria y en la Escuela Nacional de Estudios Profesionales Plantel Aragón (ENEP Aragón). El plan de estudios de la ENEP Aragón fue aprobado el 11 de marzo de 1992 por el H. Consejo Universitario y consta de 10 semestres con un total de 418

créditos que el alumno deberá cubrir con base en cursar y acreditar 50 materias, cuatro de ellas optativas. El último semestre comprende la materia de redes de computadoras.

Esta materia es impartida 4 horas a la semana, durantes 16 semanas lo que nos da un total de 64 horas divididas en 6 principales temas o capítulos. Los capítulos pueden verse en la Tabla 6.

TEMA	HORAS DE TEORIA
Conceptos Básicos.	9
Componentes de las Redes.	14
Procedimientos para control de enlace y transferencia de datos.	12
Asignación de capacidades en los enlaces.	10
Nodos o conmutadores de paquetes.	10
Redes y procedimientos.	9

Tabla 6. Temario de las asignaturas redes de computadoras de Ingeniería en Computación. Impartida en la ENEP Aragón.

Entre los temas que el ANIEI sugiere y que el programa de redes de computadoras que la ENEP Aragón no presenta son:

- Frame Relay y ATM
- Internet
- Ipv6
- Teoría de enrutamiento
- Optimización de redes.
- Subredes y Máscaras.
- Unix
- Aplicaciones, consultas compartidas.
- Estándares IEEE.
- Sistemas Operativos de red

Consideramos que la lista anterior muestra los principales temas que no están incluidos en el programa de redes de la ENEP Aragón. Se consideran importantes por tratarse de tecnologías nuevas o de subtemas que no se tocan a fondo en la teoría y que sin embrago son parte para complementar otros temas.

Existen temas que en al ANIEI se presentan y que pueden llevarse a la práctica. Así habría material para implementar un laboratorio que ayudaría a reforzar la materia. Estos temas son los siguientes:

- Modems.
- Métodos de transmisión serio y paralelo.

- Medios y elementos físicos.
- Dispositivos de comunicación
- Redes LAN
- Dispositivos DCE y DTE.
- TCP/IP
- Transferencia de archivos.
- Protocolos de bajo nivel: RS-232, Paralelo.
- Protocolos de alto nivel: TCP/IP.
- Internet.
- Sistemas Operativos de red.

B) Instituto Tecnológico de Estudios Superiores Monterrey.
Ingeniería en Sistemas Computacionales

Son 10 semestres los que comprenden el plan de estudios de esta carrera, en el sexto semestre se imparte la materia de Redes I, en el séptimo semestre se complementa el área con la asignatura de Redes II y por último en el octavo semestre se imparte Redes III.

Temas vistos por asignatura:

REDES I
- Modelo de comunicación de datos.
- Comunicación de datos.
- Estándares.
- Modelo OSI.
- TCP/IP y SNA.
- Señalización Digital y Analógica, Multiplexeo.
- Medios de transmisión, Topologías y Cableado Estructurado..
- Atenuación y Ruido.
- Control de Acceso al medio, detección y corrección de errores, Control de flujo.
- Técnicas de conmutación.

REDES II
- Teoría de Fila de Espera, protocolos de Nivel de Red, Ruteadores.
- Protocolos de Enrutamiento, Algoritmos de enrutamiento estático y dinámico.
- Control de congestión.
- Servicios orientados a conexión y no conexión.
- Servicios de la capa de transporte.
- Servicios de la capa de sesión.
- Servicios de la capa de presentación, representación de datos.
- Compresión de datos, encriptación, Autentificación.

REDES III

- Aplicaciones de Red HTTP, SMTP, TELNET, SNMP, FTP.
- Diseño de redes LAN y WAN.
- Desempeño de redes.
- Administración de una Red.
- Seguridad en redes.
- ISDN, ATM, Frame Relay, Intranets y Nuevas tecnologías.

C) Instituto Politécnico Nacional
Ingeniería en Sistemas Computacionales.

Son ocho semestres lo que dura esta carrera y en quinto semestre se imparte la metería de redes de computadoras con un total de 6 créditos. Su temario es el siguiente:

- Introducción
- Capa física.
- Capa de acceso al medio
- Capa de enlace de datos.
- Capa de red
- Capa de transporte.
- Capas superiores.
- Redes Comerciales de Computadoras.

D) Universidad del Valle de México

Son dos carreras que imparten esta Universidad Ing. En Computación y Lic. Sistemas de Computación Administrativa donde son tres semestres que toman la materia de Redes de Computadoras y es exactamente el mismo temario de esta materia para ambas carreras .Temas vistos por asignatura:

REDES I

- Modelo de comunicación de datos.
- Comunicación de datos.
- Estándares.
- Modelo OSI.
- TCP/IP y SNA.
- Señalización Digital y Analógica, Multiplexeo.
- Medios de transmisión, Topologías y Cableado Estructurado..
- Atenuación y Ruido.
- Control de Acceso al medio, detección y corrección de errores, Control de flujo.
- Técnicas de conmutación.

REDES II

- Teoría de Fila de Espera, protocolos de Nivel de Red, Ruteadores.
- Protocolos de Enrutamiento, Algoritmos de enrutamiento estático y dinámico.
- Control de congestión.
- Servicios orientados a conexión y no conexión.
- Servicios de la capa de transporte.
- Servicios de la capa de sesión.
- Servicios de la capa de presentación, representación de datos.
- Compresión de datos, encriptación, Autentificación.

REDES III

- Aplicaciones de Red HTTP, SMTP, TELNET, SNMP, FTP.
- Diseño de redes LAN y WAN.
- Desempeño de redes.
- Administración de una Red.
- Seguridad en redes.
- ISDN, ATM, Frame Relay, Intranets y Nuevas tecnologías.

Es de suma importancia mencionar que de las cuatro Instituciones de las cuales se analizaron sus planes de estudio, tres de ellas cuentan con un laboratorio de Redes y telecomunicaciones por lo tanto de esas cuatro la única que no cuenta con un laboratorio oficial de Redes o Telecomunicaciones es la Escuela Nacional de Estudios Profesionales plantel Aragón.

Cabe mencionar que la Universidad del Valle de México y el Instituto Tecnológico de Estudios Superiores Monterrey tienen como asignatura únicamente el laboratorio de CISCO y se les evalúa a través de un examen por red de los conocimientos adquiridos en el laboratorio virtual que CISCO les proporciona, es decir, no adquieren los conocimientos de esta asignatura a través de una clase en un aula.

Se elaboró una tabla donde se hace una comparación de los temas y subtemas de las Universidades antes mencionadas ver Anexo C.

2.3. LA IMPORTANCIA DEL LABORATORIO EN LA FORMACIÓN PROFESIONAL

2.3.1. El laboratorio

Hablando históricamente, en Europa, los laboratorios estuvieron dedicados a la alquimia y a la elaboración de productos médicos, por lo que durante mucho tiempo, el término laboratorio se reservo para los químicos o farmacéuticos. Sin embargo, en la medida en que fueron surgiendo actividades científicas se fue demandando de equipo e instalaciones especializadas donde se realizarían trabajos de física, biología, fisiología y

mineralogía, por lo que para el siglo XIX se transformo el uso del laboratorio hasta alcanzar la importancia actual[1].

El laboratorio va adquiriendo sentido y significado en la medida en que la producción del conocimiento científico requiere de un espacio para generar conocimientos. En este caso la primera exigencia metodológica de la ciencia radica en utilizar en sus enunciados, conceptos precisos mediante definiciones de operación.

El laboratorio hace referencia a un lugar donde se labora, a un espacio donde se efectúan operaciones, experimentos, en donde se amplían, desarrollan y comprueban los datos que conforman a la ciencia. El laboratorio representa al espacio en donde al irse desarrollando el uso de la ciencia se plantea la necesidad de innovarla a través de los propios laboratorios de investigación que se desarrollan. De esta manera, la importancia del laboratorio reside en que en ellos se crea la ciencia. Es ahí donde la ciencia representa sus más diversas manifestaciones.

Revisando la historia, se encontró que en la edad media los laboratorios se constituyeron como los lugares donde se podían poner a prueba las ideas que se generaban con base en la observación cotidiana. Se consideró también que los laboratorios respondían, en ese momento, a dos necesidades, la primera, para tener un lugar aislado y tranquilo donde el investigador podía probar la explicación de sus hipótesis y donde podía medir o controlar el mayor número de variables, la segunda, para que en condiciones muy bien controladas lo que parecía que sucedía en otras condiciones pudiera ser reproducido.

El primer laboratorio que hubo en México durante la época de la Colonia, centraba su actividad en la metalurgia y su principal interés era comprobar si las muestras obtenidas tenían oro y en qué proporción. Lo importante en este antiguo laboratorio era que allí se comprobara si había oro y si era productiva la mina recién descubierta. Aquí los alumnos deberían de capacitarse y aprender a comprobar. Más tarde, en la medida en que la ciencia fue ampliando su campo e incursionando en el espacio educativo, los laboratorios comenzaron a adquirir gran importancia y fueron considerados como salones de comprobación de conocimientos. Estro fue útil en los primeros años en las escuelas y universidades, al irse generando cada vez más conocimientos, la validez de este concepto del laboratorio como lugar de comprobación ya no pudo sostenerse y se le otorga un sentido que indica que el laboratorio permite al alumno lograr un "refuerzo del conocimiento teórico". Sin embargo, recientemente se ha planteado la situación de que son múltiples las ramas de la ciencia, que avanza con base en los laboratorios cada vez más especializados, de tal manera que en la actualidad es sumamente difícil contar con laboratorios adecuados para reforzar los conocimientos en las diferentes ramas de la ciencia.

Se puede decir que el laboratorio es uno de los principales espacios de formación en el cual el alumno aplica el método científico. El proceso enseñanza aprendizaje se

[1] U.T.H.E.A., (1983), *Diccionario Enciclopédico, México*, U.T.H.E.A, p.768.

desarrolla en base en la solución de problemas[2] con la idea de desarrollar mecanismos pedagógicos como son la curiosidad del alumno, su capacidad para identificar hechos, su capacidad para observar y su capacidad para formular preguntas y buscar soluciones. Aquí la intención es que el alumno aprenda a planear ordenada y cuidadosamente sus actividades, que adquieran el hábito de conducir su trabajo de acuerdo a una o varias hipótesis, que interpreten críticamente los hechos y que asienten por escrito y fielmente los avances de su experimento.

Por lo tanto el laboratorio no es un espacio o extensión del aula sino un espacio de formación donde se trabaja permanentemente, creándose un ambiente que favorece los procesos de interacción, intercambio y formación de los investigadores. En el laboratorio se fomenta uno de los elementos primordiales de la formación científica que es el desarrollo de la capacidad creativa y crítica para resolver problemas de investigación; por eso se puede decir que un investigador en formación, entre otras cosas, debe ser una persona capaz de aplicar sus conocimientos y métodos en la solución de nuevos problemas, porque para la solución de esos problemas necesita capacidad de razonamiento, establecer los procedimientos de producción para contribuir al descubrimiento de aparatos y por lo tanto hacer aportaciones a la ciencia pura o aplicada.

En el mismo orden de ideas el estudiante se ve en la necesidad de aplicar una o algunas metodologías para la solución de problemas, desde los conceptos y situaciones más sencillas hasta las más complejas y elaboradas; se trata aquí de que el estudiante no sólo revise procesos, sino más bien de que desarrolle al mismo tiempo sus habilidades para aplicarlos.

Para complementar la noción histórica del laboratorio se han recuperado algunos planteamientos de Burton Clark sobre el contexto europeo de la adopción del laboratorio en el espacio universitario. Este autor señala que la reforma universitaria alemana en los albores del siglo XIX, se relaciona con el nombre de Wilhelm Von Humboldt [3], quien estableció como principio la unidad entre investigación, docencia y estudio. Expresada de diversas maneras en Alemania y el resto del mundo, esta ideología académica estableció premisas que vinculan la producción y divulgación del conocimiento. Por ejemplo, que quienes enseñan en los niveles avanzados del sistema educativo dedicados a ellos mismos a la investigación deben entrenar a los estudiantes para la investigación haciéndolos participar en la misma. Por lo que en los laboratorios

[2] La solución de problemas, en términos generales, se refiere a la obtención de datos significativos a partir de una pregunta y, a la aplicación de esos resultados a fin de lograr la respuesta apropiada. Representa a su vez, la adopción de una estrategia de investigación.

[3] "...El principio humboldtiano se volvió muy influyente en el desarrollo de la educación avanzada a finales del siglo XIX y en el siglo XX en la mayor parte de las naciones avanzadas, y represento un concepto particularmente dominante primero en las universidades alemanas y después en las estadounidenses. Por bastante mas de un siglo, el concepto ha expresado amplia y concretamente en el uso organizacional del seminario y laboratorio de docencia e investigación como vehículos primarios de la educación avanzada" Clark, Burton (1997), *Las universidades modernas: espacios de investigación y docencia*, México, Coordinación de Humanidades/Porrúa, p.10.

y seminarios, los estudiantes se vuelven investigadores al buscar propuestas a problemas de investigación que los profesores especifican o que ellos mismos plantean.

Siguiendo con esta argumentación, en este proceso los profesores y estudiantes se vuelven colegas de investigación y unen sus esfuerzos en una búsqueda común de la verdad representada por un nuevo conocimiento; aquí la investigación se transforma en un modo de estudio, y en una modalidad de formar a los futuros investigadores. En este modelo de enseñanza el alumno aprende al lado de su tutor, que es un investigador productivo en determinada línea de investigación, por lo que esta educación basada en la investigación tiene semejanza con la organización moderna de las universidades.

Por otro lado, ante el propósito de promover en las universidades una formación basada en la investigación. Clark señala que a partir de la segunda mitad del siglo XX se ha desarrollado en todo el muerdo una compleja relación entre educación e investigación. Por ejemplo, al haberse incrementado la escala de operaciones desde la Segunda Guerra Mundial, cada ámbito se hizo más dependiente del patronazgo financiero gubernamental, situación que dio lugar a una relación más complicada entre un sistema de investigación, un sistema de educación avanzada (de posgrado) y un sistema de financiamiento. Ocurrió que, el sistema de investigación se ha extendido cada vez más por laboratorios gubernamentales, industrias e instituciones no lucrativas así como un número mayor de instituciones de educación superior.

Clark plantea que antes de las demandas del contexto "...las universidades alemanas desarrollaron y expresaron una visión investigativa en nuevas herramientas organizacionales como el laboratorio de enseñanza a través de la investigación y el seminario orientado a la investigación. En términos genéricos, el grupo académico de investigación nació y después se institucionalizó en forma de instituto, como unidad básica de organización, al tiempo en que permitió que surgiera una nueva clase de académico: el académico disciplinario de la investigación. Esta nueva categoría se basó en el pensamiento humboldtiano para sistematizar su causa. La competencia entre las universidades descentralizadas favoreció a los nuevos académicos quienes ejemplifican la capacidad para la investigación al crear reputaciones basadas en su producción investigativa y un entrenamiento de vanguardia de los estudiantes avanzados en relaciones íntimas entre mentor y aprendiz"[4].

Todo comenzó en Alemania a principios del siglo XIX, ya que fue allí donde la ideología y los intereses se unieron poderosamente y de manera razonable para convertir la investigación en un fenómeno universitario. Fue allí en donde se estableció por vez primera el principio de una unidad de investigación y docencia. En su forma humboldtiana pura, la concepción alemana planteaba que los profesores universitarios se convirtieran en investigadores. Sus alumnos, futuros, doctores, maestros, funcionarios públicos o académicos, también deberían participar en la investigación. Juntos maestro y alumno buscarían la verdad. Lo anterior se vio reflejado en el

[4] Clark, Burton (1997), *Las universidades modernas: espacios de investigación y docencia*, México, Coordinación de Humanidades/Porrúa, p.12.

currículo, el cual tendría que ser muy flexible y dependería de los profesores y estudiantes. Ambos decidirían qué trabajar y realizarían sus propias indagaciones. De esta manera, los estudiantes se vieron liberados y las opciones tanto como para los profesores y estudiantes se ampliaron. De esta manera, profesor y estudiante, trabajarían en el desarrollo del conocimiento científico.

El laboratorio universitario comienza a jugar un papel muy importante, tanto que "...se convirtió en la herramienta organizacional del profesor-científico; en su interior se desarrollaron y llevaron a cabo los procedimientos de entrenamiento; se establecieron las calificaciones de especialistas que certificaban la competencia científica pasó a ser para la ciencia el equivalente del estudio del artista renacentista, que permitía a los aprendices integrase a la sociedad científica por medio del hospedaje en habilidades prácticas bajo la dirección de un maestro-practicante. El laboratorio universitario alemán se convirtió en el lugar en donde los estudiantes que habían conocido la gramática de la ciencia en conferencias aprendían su lenguaje en la experiencia práctica..."[5] .

2.3.2. La enseñanza de la ciencia en el laboratorio

De entrada, no se puede pensar en la enseñanza de las ciencias sin considerar un laboratorio, es como pensar en una empresa sin futuro. El laboratorio a través de la historia ha sido considerado como una pieza fundamental en la enseñanza y los avances de las diferentes ciencias; en él, se practicaban las teorías, las hipótesis, se reproducían fenómenos bajo condiciones muy controladas, se hacían experimentos de demostración.

En el laboratorio desembocan varios intereses uno que hace referencia a un proceso formativo que se caracteriza por introducir de manera natural al alumno al aprendizaje del método científico. En este proceso el alumno es preparado para estudiar nuevas situaciones a partir del planteamiento de un problema y la búsqueda de nuevas soluciones. Otro de los intereses es informativo. En el laboratorio, a través del trabajo experimental se fomenta la discusión y el intercambio de ideas, esto genera que las relaciones entre estudiantes y profesores sean más estrechas y estén más consolidadas para el trabajo de investigación que se pretende desarrollar. Cuando estos dos intereses se articulan el trabajo de laboratorio cumple el requisito de ser formativo, pues desarrolla y estimula el sentido crítico del estudiante, de esta manera el estudiante adquiere métodos, hábitos y habilidades que el trabajo de laboratorio requiere para ser satisfactorio.

El laboratorio ofrece también al estudiante una cultura científica, una estructura social y un sistema de normas, valores, costumbres y jerarquías que son creadas por los equipos de investigación y que son impuestas de manera implícita a través de las interacciones diarias, los intercambios, el trabajo en equipo.

---

[5] Clark, Burton (1997), *Las universidades modernas: espacios de investigación y docencia*, México, Coordinación de Humanidades/Porrúa, p.21.

En otro orden de ideas, pero no menos importante, el laboratorio juega un papel importante en el desempeño de la investigación experimental y en el aspecto didáctico.

Ambos aspectos articulan y dan como resultado la creación de la ciencia a través del recurso didáctico que representa el laboratorio y que resulta fundamental en el aprendizaje de la ciencia. Por lo tanto el laboratorio resulta ser el lugar ideal para aprender a resolver problemas, aplicar las metodlogías más adecuadas para resolver los problemas de investigación. Se resuelven desde problemas sencillos hasta los más complejos.

El trabajo experimental que desarrolla en el laboratorio es muy riguroso y equivale al 90% de las actividades que desempeñan los estudiantes para su formación como investigadores, de igual manera las exigencias que se les hacen a los estudiantes son muy estrictas. El estudiante debe tener una gran capacidad inventiva y manual para enfrentarse a los problemas de investigación, tiene que resolver los problemas con inteligencia y creatividad.

En el laboratorio los estudiantes se forman trabajando, todo es sobre la marcha, en la investigación experimental el laboratorio es la base de la enseñanza. La manera en que se aprende se lleva a cabo en el momento de resolver problemas específicos. La idea es encontrar la información que le sirva para resolver y llevar a cabo el experimento.

Actualmente en muchas industrias y en los posgrados de ciencias experimentales, el laboratorio es una de las piezas fundamentales de la organización colegiada e industrial; de ahí que los laboratorios de investigación sean indispensables para el avance y progreso de todas las ciencias experimentales.

A través de la historia los laboratorios son considerados como una pieza primordial en la enseñanza de las ciencias. Se puede plantear que sin los laboratorios simplemente no se daría el proceso de enseñanza y de aprendizaje. En él se encuentran las condiciones humanas y materiales para fomentar y promover la enseñanza del oficio de investigador en las ciencias experimentales.

2.4. INVESTIGACIÓN DE UN LABORATORIO DE REDES EN LA ENEP ARAGÒN

A continuación se describe el trabajo de investigación que se realizó en la ENEP Aragón y las estadísticas que señalan la importancia de implementar un laboratorio de Redes de Computadoras.

Esta investigación se hizo en base a un cuestionario dirigido a los profesores que actualmente imparte esta materia, a los alumnos que se encuentran cursando la materia y a alumnos que han terminado la carrera y que se encuentran trabajando actualmente en el área de redes (Ver anexo C).

Dentro de los principales factores que se analizaron se encuentran los siguientes:

- *El lugar*, con lo que respecta a este punto se tiene contemplado utilizar un lugar apropiado y con las instalaciones adecuadas, se puede tomar como arquetipo el laboratorio de Comunicaciones Digitales ya que es lugar amplio y cuenta con las instalaciones apropiadas para correcto desempeño. De igual forma es importante mencionar que actualmente se cuenta con un laboratorio de Redes que se encuentra ubicado en el salón A5034 Centro de Apoyo a Estudiantes, donde se cuenta con muy poco material y recursos, este material a sido de alguna u otra forma donado por los alumnos a través de prácticas que han llevado a cabo ahí y se de esa forma se ha ido recopilando material para su uso posterior con otros alumnos. El espacio de trabajo de este laboratorio es muy reducido y el instructor que actualmente imparte las prácticas se ha visto en la necesidad de dividir al grupo y a su vez trabajar en equipo, ya que de otra forma las herramientas y el material serian insuficientes.

- *Material y recursos*, como se menciono a grandes rasgos en el punto anterior, la gran mayoría del material con que cuenta actualmente el laboratorio ha sido donado por los alumnos que han tomado prácticas en este laboratorio. Algunos recursos han sido donados por empresas y muchos otros han sido adquiridos por el propio laboratorio con fondos que fueron recabados a través de cursos impartidos a la comunidad estudiantil.

  Algunos recursos con los que cuenta actualmente el laboratorio se listan a continuación:

  - 3 routers Cisco serie 1700 modelo 1720.
  - 1 router Cisco 1700 modelo 1750.
  - 1 switch Catalyst 2950.
  - 3 equipos Pentium 4 sistema operativo Windows 98, XP y 2000.
  - 2 pinzas para ponchado de cable UTP.
  - Escáner para verificar conectividad de cables UTP.
  - Hub de 8 puertos.
  - 2 Access Point
  - 1 NBX (Dispositivo para trabajar con voz sobre IP).
  - 2 teléfonos IP.

- *El personal*, en cuanto a este punto la escuela cuenta con bastante personal que puede hacerse cargo de la instalación y el mantenimiento del laboratorio, este personal estará conformado por los alumnos que hacen su servicio social en el área de Redes y que actualmente lo hacen en el centro de Apoyo a Estudiantes, estos alumnos serán capacitados para poder llevar a cabo el proceso de la instalación del laboratorio y posteriormente de su mantenimiento, de esta forma

la escuela no tiene que hacer un gasto en la contratación de personal y ese capital se podría invertir en la adquisición de nuevo material.

Algunos de los profesores que se les menciono a cerca de este proyecto les interesa estar personalmente involucrados dentro del desarrollo de este laboratorio, ya sea como instructores impartiendo el laboratorio o creando nuevas prácticas para el temario; algunos otros profesores les interesa solo en el plano que corresponde a la elaboración de material para la realización de las prácticas.

- *Implementación,* este punto va relacionado mucho con el punto anterior, ya que la implantación del laboratorio será realizado por el personal del que se hizo mención en el punto del personal. Esta es una buena forma de hacer uso de los recursos humanos con los que cuenta la escuela a parte de que es un beneficio para todos aquellos alumnos que les interese formar parte de este proyecto ya que se verán involucrados directamente y esto ampliara sus conocimientos dentro del área. Es importante mencionar que todo aquel personal que formara parte del laboratorio será capacitado por personal experto en el tema.

- *Prácticas,* este punto es uno de los más importantes ya que de nada serviría toda una infraestructura sino se cuenta con las prácticas que avalaran su correcto desempeño, logrando cubrir sus objetivos como laboratorio y satisfaciendo las necesidades de la comunidad estudiantil en el área de Redes. Actualmente el instructor del laboratorio de Redes que se localiza en el Centro de Apoyo a Estudiantes ha desarrollado una serie de prácticas y es precisamente este trabajo de tesis que apoya la creación de más prácticas, en este caso y siendo más específicos a la parte del temario que corresponde al protocolo de comunicación TCP/IP.

- *Rentabilidad,* en cuanto a este punto, es importante señalar que una vez instalado el laboratorio se requerirá de capital para su posterior mantenimiento y actualización de los recursos. Al ser un laboratorio donde el hardware es de suma importancia y la frecuencia con la que se va mejorando es constante, se deberá ir actualizando el laboratorio teniendo hardware de vanguardia, de esta manera los alumnos tendrán conocimientos de redes actualizados y no conocimientos que ya no son aplicables. La escuela a través de este laboratorio pude impartir cursos inter semestrales a estudiantes que ya cursaron la materia de Redes y por ende el laboratorio, pero que quieren actualizar sus conocimientos o profundizar un poco más en ellos, de esta forma el laboratorio al cobrar una mínima cantidad podrá mantenerse por si solo, otro punto sería que este mismo laboratorio se impartiera a personas externas donde obviamente el costo aumentaría , y de esta forma el laboratorio tendría con que solventar sus propios gastos.

Conclusiones

Tomando en cuenta las respectivas respuestas de cada uno de los profesores se llegó a la conclusión de que haría falta personal capacitado para impartir el laboratorio, ya que no todos los profesores cuentan con el tiempo suficiente para impartirlo.
Algo importante en este análisis es que los profesores si tienen el interés absoluto de que se imparta el Laboratorio de Redes y algunos cuentan con el tiempo necesario para poder hacerlo.

Es importante señalar que los pocos profesores que si podrían lo hacen por el solo interés de que el alumnos salga de la carrera capacitado con el fin de llegar con las habilidades y conocimientos necesarios para poder desempeñar al 100% su trabajo dentro del sector laboral.

Evaluando las respuestas dadas por los alumnos a los cuestionarios aplicados, se refleja un gran interés en la creación urgente de un laboratorio de redes, ya que para todos es fundamental reafirmar los conocimientos de la materia de forma tangible, pues es una área muy importante y extensa dentro de la ingeniería en computación y la mayoría coincide en que es fundamental para su desempeño laboral, aun no especializándose en esa área (ver Anexo C).

Un factor muy importante es la aportación que están dispuestos a dar los alumnos, que es el apoyo económico, con el cual se obtendrá la tecnología necesaria para la implementación de dicho laboratorio.

La gráfica muestra el bajo porcentaje de alumnos (solo 2/50) que no están interesados en cursar el laboratorio de redes, básicamente sus argumentos fueron los siguientes:

- Perdida de tiempo
- El personal que imparte el laboratorio no esta capacitado.
- Falta de recursos tanto tecnológicos como económicos, para poder realizar las practicas.
- Falta de prácticas bien estructuradas.
- Falta de tiempo.
- No están interesados en el área de redes.

La mayoría de estas opiniones son validas, pero fácilmente se pueden cambiar si se tiene el apoyo y los recursos necesarios para la creación de un laboratorio de redes, desde las practicas correctas, hasta personal capacitado y el equipo necesario, para que no sea considerado una perdida de tiempo, y despierte el interés de los alumnos sea cual sea su área de desarrollo.

De esta manera finalizamos el desarrollo del capitulo "Análisis de la materia de Redes de computadoras", y damos inicio al capitulo tres, en el cual se presenta nuestra propuesta de practicas referente a los protocolos TCP/IP, basándonos en el temario de

dicha materia presente en la E.N.E.P. Aragón. Las prácticas se exponen con un formato fácil de desarrollar, iniciando con su duración, los objetivos que se pretenden cubrir con su desarrollo, un cuestionario preliminar, cuyo fin es actualizar los conocimientos del tema en el estudiante, así como un marco teórico del tema. Las herramientas y recursos necesarios para su desarrollo. El desarrollo de la práctica se presenta por pasos y explicación de cada uno de estos, para su fácil comprensión y desarrollo, así como posibles instrucciones en algunos pasos. Pueden presentar una evaluación, para verificar que el alumnos haya comprendido el tema, tanto teórica como prácticamente, y finalmente concluimos cada práctica con las conclusiones, las cuales son a las que el alumno llego al terminar el desarrollo de cada una de las prácticas.

Capítulo 3

Propuesta de las prácticas del Protocolo TCP/IP

A continuación se presenta la propuesta de prácticas que corresponden a la parte del temario que estudia el protocolo de comunicaciones TCP/IP de la asignatura de Redes de Computadoras para un laboratorio de redes de la carrera de Ingeniería en Computación en la Escuela Nacional de Estudios Profesionales plantel Aragón.

PRÁCTICA 1 –DIRECCIONAMIENTO IP
(Duración estimada: 60 minutos)

Objetivos:

- Nombrar las cinco clases diferentes de direccionamiento IP.
- Describir las características y el uso de las diferentes clases de las direcciones IP.
- Identificar la clase de una dirección IP basándose en el número de red.
- Determinar qué parte (octeto) de una dirección IP es el ID de red, y qué parte es el ID de host.
- Identificar las direcciones de host IP válidas y no válidas basándose en las reglas del direccionamiento IP.
- Definir el rango de las direcciones y de la máscara de subred predeterminada para cada clase.

Cuestionario Preliminar

1. ¿De qué manera son nombrados los servidores y las estaciones de trabajo en una red TCP/IP?
2. En su forma más básica ¿cuáles son las dos partes que componen una dirección IP?
3. ¿Qué es el Internet Network Information Center (InternetNIC)?
4. ¿Qué es y como funciona un router (ruteador o encaminador)?
5. ¿Qué es una dirección lógica y una dirección física?
6. ¿Cuáles son las cinco clases de direcciones IP y sus estructuras?
7. ¿En qué capa del modelo OSI se encuentra el protocolo TCP/IP?

Marco Teórico

Esta práctica le ayudará a desarrollar y comprender las direcciones IP, y cómo operan las redes TCP/IP. Las direcciones IP se emplean únicamente para identificar redes y hosts TCP/IP (computadoras e impresoras) en dichas redes para que se puedan comunicar los dispositivos. Las estaciones de trabajo y los servidores de una red TCP/IP se llaman hosts, y cada uno tiene una dirección IP única, conocida como su dirección de host. TCP/IP es el protocolo más ampliamente utilizado en todo el mundo. Internet, o la World Wide Web, sólo utiliza el direccionamiento IP. Para que un host pueda acceder a Internet, debe tener una dirección IP.

En su forma básica, la dirección IP tiene dos partes: una dirección de red y una dirección de host. La parte de la red de la dirección IP es asignada a una empresa u organización por el Internet Network Information Center (InternetNIC). Los routers usan las direcciones IP para mover paquetes de datos entre redes. Las direcciones IP tienen una longitud de 32 bits (en la versión actual IPv4), y están divididas en 4 octetos de 8 bits. Operan en la Capa 3 del modelo OSI (la capa de red del modelo TCP/IP), y las asigna estáticamente (manualmente) el administrador de red, o dinámicamente (automáticamente) el servidor del protocolo de configuración dinámica del host (DHCP). La dirección IP de una estación de trabajo (host) es una "dirección lógica", lo que significa que se puede cambiar. La dirección MAC de una estación de trabajo es una "dirección física" de 48 bits, que se integra en la NIC y no se puede cambiar hasta que ésta se sustituya. La combinación de dirección lógica IP y dirección física MAC ayuda a los paquetes a llegar al destino adecuado.

Existen cinco clases de direcciones IP y, dependiendo de cómo sean la parte de red y de host de las direcciones, usarán un número de bits diferentes. En esta práctica trabajará con diferentes clases de direcciones IP, y se familiarizará con sus características. Comprender las direcciones IP es básico para entender TCP/IP y las redes en general.

Herramientas y Recursos

Éste es principalmente un ejercicio escrito, pero deberá utilizar Panel de control, Red para comprobar alguna dirección IP de la red.

Desarrollo

Paso 1. Revise las clases y características de las direcciones IP.

Explicación: existen cinco clases de direcciones IP (Figura1) (de la A hasta la E). Solo las primeras tres clases se utilizan comercialmente. Explicaremos una dirección de Clase A de la tabla para empezar. La primera columna es la clase de dirección IP. La segunda es el primer octeto, que debe encontrarse dentro del rango de una clase o dirección dadas. La dirección Clase A debe comenzar con un número entre 1 y 126. El primer bit de una dirección de Clase A siempre es cero, que significa que el Bit de orden superior (HOB) o los 128 bits no se pueden utilizar. 127 bits están reservados para las pruebas loopback. El primer octeto aislado define el ID de red para una dirección de red de Clase A. La máscara de red predeterminada utiliza sólo unos binarios (se corresponden con el numero decimal 255) para enmascarar los primeros 8 bits de la dirección de Clase A. Esta máscara ayuda a determinar a los routers y hosts si el host de destino está en esta red o se encuentra en otra. Ya que sólo hay 126 redes de Clase A, los restantes 24 bits (3 octetos) se pueden emplear para los hosts. Cada red de Clase A puede tener 2^{24} hosts, es decir, unos 16 millones de hosts. Es muy común subdividir la red en grupos más pequeños que se llaman subredes utilizando una máscara de subred personalizada, sobre la que hablaremos en la siguiente práctica.

La parte de red o host de la dirección no puede estar formada completamente por unos o ceros. Como en el ejemplo, la dirección de Clase A 118.1.1.5 es una dirección IP válida, porque la parte de red (primeros 8 bits, igual a 118) no son todo ceros, y la parte host (los últimos 24 bits) no son todos ceros o unos. Si la parte de host fuese todos ceros, sería la dirección de red en sí misma, y si fuese todos unos, sería una difusión para la dirección de red. El valor de cualquier octeto no puede ser nunca mayor que el decimal 255 o el binario 11111111.

Clase	Rango decimal Del primer octeto	Bits de Orden Superior Del primer Octeto	ID de Red/host (R= red, H= host)	Máscara De subred predeterminada	Número de redes	Hosts Por red (direcciones utilizables)
A	1-126*	0	R.H.H.H	255.0.0.0	126 (2^7-2)	16.777.214 (2^{24}-2)
B	128-191	10	R.R.H.H	255.255.0.0	16.382 (2^{14}-2)	65.534 (2^{16}-2)
C	192-223	110	R.R.R.H	255.255.255.0	2.097.150 (2^{21}-2)	254 (2^8-2)
D	224-239	1110	Reservada par la multidifusión.			
E	240-254	11110	Experimental ;usada para investigación			

Figura 1. *La dirección 127 de Clase A no se puede usar y está reservada para funciones de loopback y diagnóstico.

Paso 2. Direccionamiento IP básico.

Instrucciones: utilice el mapa de direcciones IP y sus conocimientos sobre las clases de direcciones IP para responder a las siguientes preguntas.

1. ¿Cuál es el rango decimal y binario del primer octeto de todas las posibles direcciones IP de Clase B?

Decimal: Desde: _____ hasta: _____
Binario: Desde: _____ hasta: _____

2. ¿Qué octeto(s) representa(n) la parte de una dirección IP de Clase C?_____
3. ¿Qué octeto(s) representa(n) la parte de host de una dirección IP de Clase A?_____

Paso 3. Determine las partes de host y de red de las direcciones IP.

Instrucciones: en las siguientes direcciones IP de host, indique la clase de cada una, la dirección o ID de red, la parte de red, la dirección de difusión para esta red y la máscara de subred predeterminada.

Explicación: la parte de host para ID de red estará formada completamente por ceros. Introduzca sólo los octetos que crean el host. La parte de host para la difusión estará formada totalmente por unos. La parte de las direcciones para la máscara de subred estará formada por unos.

1. Rellene la siguiente tabla:

Dirección Ip de host	Clase de dirección	Dirección de red	Dirección de host	Dirección de difusión De red	Máscara De subred Predeterminada
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.44					

2. Dada la dirección IP 142.226.1.15,

a. ¿Cuál es el binario equivalente del primer octeto?_____
b. ¿Cuál es la clase de la dirección?_____
c. ¿Cuál es la dirección de red de esta dirección IP?_____
d. ¿Es ésta dirección IP de host válida (S/N)?_____
e. ¿Por qué o por qué no?_____
_____
_____
_____

3. ¿Cuál es el número máximo de host que puede tener con una dirección de red de Clase C?_____

4. ¿Cuántas redes de Clase B existen?_____

5. ¿Cuántos host pueden tener las redes de Clase B?_____

6. ¿Cuántos octetos hay en una dirección IP?_____¿Cuántos bits por octeto?_____

Paso 4. Determine qué direcciones IP de host son válidas para las redes comerciales.

Instrucciones: para las siguientes direcciones IP de host, determine ¿cuáles son válidas para las redes comerciales. ¿Por qué si o por qué no?

Explicación: válida significa si se puede asignar a una estación de trabajo, servidor, impresora, interfaz de router, etc.

1. Rellene la siguiente tabla.

Dirección IP de host	¿Dirección correcta?(si/no)	Por qué sí o por qué no
150.100.255.255		
175.100.255.18		
195.234.253.0		
100.0.0.23		
188.258.221.176		
127.34.25.189		
224.156.217.73		

Conclusiones

Que el alumno describa una breve conclusión a la que haya llegado a cerca del estudio de las diferentes clases de direcciones IP.

PRÁCTICA 2– SUBREDES
(Duración estimada: 60 minutos)

OBJETIVOS

- Que el alumno comprenda la definición de subneteo.
- Que el alumno aprenda a realizar tablas de subneteo.
- Que el alumno aprenda a interpretar las tablas de subneteo.
- Que el alumno aprenda a resolver problemas reales por medio de tablas de subneteo.

CUESTIONARIO PRELIMINAR

1. Menciona cuales son las cinco clases de direcciones IP y sus rangos y restricciones
2. ¿Qué es una subred?
3. ¿En que consiste el termino subneteo?
4. Explique con sus propias palabras la necesidad de "subdividir" una red.
5. Investigue en que consisten los siguientes términos:

a) Peticiones ARP.
b) Envíos RIP.
c) Peticiones DNS.

6. Explica la razón por la que no se pueden utilizar lás siguientes direcciones.

a) 0000 0000
b) 1111 1111
c) 0111 1111

MARCO TEÓRICO

Hoy en día la creación de subredes a partir de una dirección IP y su mascara correspondiente, es conocido como "Subnetting" o "Subneteo", hecha la aclaración se usara este termino en lo subsiguiente de la practica.
La necesidad del subnetear una red IP puede deberse a diversos factores, que incluyen la ubicación geográfica de los nodos de la empresa, el uso de diferentes tecnologías (Ethernet, FDDI, Token Ring, Frame relay, etc), hace eficiente el direccionamiento IP o por las políticas de seguridad La razón mas común, es controlar el trafico de la red. En una red Ethernet, los nodos en un segmento, ven el trafico generado por todos los nodos

pertenecientes al segmento, el desempeño de esta red puede verse afectado por altas cargas de trafico o colisiones que provocan retransmisión de tramas.

Cuando se trabaja con una red pequeña, con pocos host conectados, el administrador de red puede fácilmente configurar el rango de direcciones IP usado para conseguir un funcionamiento óptimo del sistema. Pero conforme la red va creciendo se hace necesaria una división en partes de la misma.

En primer lugar, porque conforme se va extendiendo la red va aumentando de forma pareja el dominio de colisión, llegando un momento en el que el rendimiento de la red se ve afectado seriamente. Esto se puede mitigar segmentando la red, dividiendo la misma en una serie de segmentos significativos, de tal forma que mediante switches podremos limitar estos dominios de colisión, enviando las tramas tan sólo al segmento en el que se encuentra el host destino.

En segundo lugar, y, esto es aunque segmentemos la red, conforme aumenta el número de host aumenta también el número de transmisiones de broadcast (cuando un equipo origen envía datos a todos los dispositivos de la red), llegando un momento que dicho tráfico puede congestionar toda la red de forma inaceptable, al consumir un ancho de banda excesivo. Esto es así porque todos los host están enviando de forma constante peticiones de este tipo: peticiones ARP, envíos RIP, peticiones DNS, etc.

Para solventar este hecho es preciso dividir la red primaria en una serie de subredes, de tal forma que cada una de ellas va a funcionar luego, a nivel de envío y recepción de paquetes, como una red individual, aunque todas pertenezcan á la misma red principal (y por lo tanto, al mismo dominio). De esta forma, aunque la red en su conjunto tendrá una dirección IP única, a nivel administrativo podremos considerar subredes bien diferenciadas, consiguiendo con ello un control del tráfico de la red y una limitación de las peticiones de broadcast que la atraviesan.

HERRAMIENTAS Y RECURSOS

Éste es principalmente un ejercicio escrito, pero deberá utilizar Panel de control, Red para comprobar alguna dirección IP de la red.

DESARROLLO

Paso 1: Revise las direcciones utilizables por red.

Explicación: Recordando lo visto en la practica 1, existen 5 clases de direcciones IP.

Redes clase A: utilizan sólo el primer byte como dirección de red y tres para direcciones de estación. Se utilizan para redes muy grandes, ya que pueden albergar 16.777.214 estaciones. Se las identifica pues el primer bit del primer octeto es 0, es decir, las redes clase A van del 1.0.0.0 al 126.0.0.0, es decir 126 redes en total (la número 0 esta reservada para el gateway default y la 127 esta reservada para las pruebas loopback).

· Redes clase B: utilizan 2 bytes para el número de red y dos para la dirección de estación. Son redes grandes y pueden albergar 65534 estaciones. Se las identifica pues los dos primeros bits del primer byte son 10, es decir, desde la red 128.1.0.0 hasta la red 191.254.0.0.

· Redes clase C: utilizan 3 bytes para el número de red y uno para el número de estación, dando un total de 254 estaciones por red. Se identifican porque el primer byte comienza por 110, es decir que las redes clase C van desde la 192.1.1.0 hasta la 223.254.254.0

· Direcciones de clase D: ya aquí no se habla más de redes sino de grupos de direcciones. Las direcciones clase D fueron definidas para grupos multicast, es decir, un paquete transmitido por una estación es recibido por todas las estaciones que comparten esta dirección multicast. Esto es muy utilizado para videoconferencias, transmisión de audio y TV por IP. Al sector de Internet que soporta multicast se lo conoce bajo el nombre de Mbone (Multicast Backbone). Esta tecnología aun no ha sido muy difundida. Las direcciones de multicast, entonces, empiezan el primer byte con 1110, es decir, van desde la dirección 224.1.1.1 hasta la 239.254.254.254.

· Direcciones clase E: están reservadas y aun no se les dio uso. Poseen los cuatro primeros bits del primer byte en 1, y van desde la 240.1.1.1 hasta la 254.254.254.254.

Paso 2: División de la dirección IP o Subneteo.

Explicación

Vamos a tomar como ejemplo una red de clase C, de la cual queremos obtener sus subredes validas y sus direcciones IP validas, teniendo claro que lo que se explique va a ser útil para cualquier tipo de red, sea de clase A, B o C. Entonces, tenemos nuestra red, con dirección IP **210.25.2.0**, por lo que tenemos para asignar a los host de la misma todas las direcciones IP del rango 210.25.2.1 al 210.25.2.254, ya que la dirección 210.25.2.0 será la de la propia red y la 210.25.2.255 será la dirección de broadcast general.

Si expresamos nuestra dirección de red en binario tendremos:

210.25.2.0 = 11010010.00011001.00000010.00000000

Con lo que tenemos 24 bits para identificar la red y 8 bits para identificar los host.

La máscara de red será:

11111111.11111111.11111111.00000000 = 255.255.255.0

Para crear subredes a partir de una dirección IP de red padre, la idea es "robar" bits a los host, pasándolos a los de identificación de red. ¿Cuántos bits? Eso depende de las subredes que se quieran obtener, teniendo en cuenta que cuántas más bits robemos, más subredes obtendremos, pero con menos host cada una. Por lo tanto, el número de bits a robar depende de las necesidades de funcionamiento de la red final.

El siguiente elemento que se debe calcular para cada una de las subredes es su máscara de subred, concepto análogo al de máscara de red en redes generales, y que va a ser la herramienta que utilicen luego los routers para dirigir correctamente los paquetes que circulen entre las diferentes subredes.

Para obtener la máscara de subred basta con presentar la dirección propia de la subred en binario, poner a 1 todos los bits que dejemos para la parte de red (incluyendo los robados a la porción de host), y poner a 0 todos los bits que queden para los host. Por último, pasaremos la dirección binaria resultante a formato decimal separado por puntos, y ésa será la máscara de la subred.

Por ejemplo, si tenemos la dirección de clase B:

150.10.x.x = 10010110.00001010.hhhhhhhh.hhhhhhhh

y le quitamos 4 bits a la porción de host para crear subredes:

10010110.00001010.rrrrhhhh.hhhhhhhh

la máscara de subred será:

11111111.11111111.11110000.000000

que pasada a decimal nos queda:

255.255.240.0

Las máscaras de subred, al igual que ocurre con las máscaras de red, son muy importantes, resultando imprescindibles para el trabajo de enrutamiento de los routers.

Paso 3. Creando las subredes.

Explicación: Vamos a partir de una dirección IP de la red padre y vamos a ir quitando bits sucesivos a la porción de host, calculando en cada caso las subredes obtenidas, sus direcciones IP, sus máscaras de subred y el rendimiento de la partición obtenida.

Para ello, pasamos la dirección IP a binario, tomamos los bits robados a la porción de host y vamos variando algunas formas posibles.

Robo de 1 bit:Si quitamos un sólo bit a la parte de host:

Parte de red: 11010010.00011001.00000010.r

Parte de host: hhhhhhh

11010010.00011001.00000010.r hhhhhhh

Permutando los bits de host robados para obtener las subredes obtenidas:

$2^1=2$

Es decir, 2 subredes (11010010.00011001.00000010.0 y 11010010.00011001.00000010.1). Pero resulta que no podemos disponer de la subred que toma el 0, ya que entonces contendría la IP de la red padre, ni de la que toma el 1, ya que contendría la dirección de broadcast de la red padre. Es decir, robando 1 sólo bit no podemos crear subredes.

NOTA IMPORTANTE: *Como regla general, el número de subredes obtenidas al quitar n bits a la porción de host será* 2^2*-2, y el número de host disponible en cada subred será* $2^{(8-n)}$*-2, ya que toda subred debe tener su propia dirección de red y su propia dirección de broadcast.*

Robo de 2 bits:

Parte de red: 11010010.00011001.00000010.rr

Parte de host: hhhhhh

11010010.00011001.00000010.rr hhhhhh

Número de subredes válidas: $2^2-2=2$

Número de host válidos por subred: $2^6-2=62$

Las direcciones de subred las obtenemos haciendo las combinaciones posibles con los 2 bits robados:

11010010.00011001.00000010. **00** 000000 a 11010010.00011001.00000010. **00** 111111 =210.25.2.0 a 210.25.2.63 (no vale, al contener la dirección de red de la red padre).

11010010.00011001.00000010.**01**000000 a 11010010.00011001.00000010.**01**111111 = 210.25.2.64 a 210.25.2.127

Subred válida, con dirección de red=210.25.2.64, broadcast=210.25.2.127 y 62 direcciones IP para host, que son las comprendidas entre las dos anteriores (de la 210.25.2.65 a la 210.25.2.126).

Máscara de subred:

11111111.11111111.11111111.11000000 = 255.255.255.192

11010010.00011001.00000010.**10** 000000 a

11010010.00011001.00000010.**10** 111111 = 210.25.2.128 a 210.25.2.191

Subred válida, con dirección de red=210.25.2.128, broadcast=210.25.2.191 y 62 direcciones IP para host, que son las comprendidas entre las dos anteriores (de la 210.25.2.129 a la 210.25.2.190).

Máscara de subred:

11111111.11111111.11111111.11000000 = 255.255.255.192

11010010.00011001.00000010.**11** 000000 a

11010010.00011001.00000010. **11111111** = 210.25.2.192 a 210.25.2.225 (no vale, al contener la dirección de broadcast de la red padre).

Resumiendo: obtenemos dos subredes válidas, con 62 direcciones IP válidas cada una, es decir, desperdiciamos:

(256-2)-(62+62)=130

130 direcciones IP para host, con lo que el rendimiento de la partición en subredes será:

R= (IP útiles subredes)/ (IP útiles totales)=124/254=0.488=48%

La máscara de subred es la misma para todas las subredes obtenidas robando 2 bits a la porción de host, y lo mismo ocurre para el robo de otro número de bits.

	Subredes	Equipos	
0	00	000000	
1	00	000001	
2	00	000010	
3	00	000011	
4	00	000100	
5	00	000101	
,			Subred invalida
,			
,			
57	00	111001	
58	00	111010	
59	00	111011	
60	00	111100	
61	00	111101	
62	00	111110	
63	00	111111	
64	01	000000	
65	01	000001	
66	01	000010	
67	01	000011	
68	01	000100	
,			No se ocupa la primera y la ultima Dicción IP de esta Subred
,			
,			
123	01	111011	
124	01	111100	
125	01	111101	
126	01	111110	
127	01	111111	
128	10	000000	
129	10	000001	
130	10	000010	
131	10	000011	
132	10	000100	
,			No se ocupa la primera y la ultima Dicción IP de esta Subred
,			
,			
187	10	111011	
188	10	111100	
189	10	111101	
190	10	111110	
191	10	111111	
192	11	000000	
193	11	000001	
194	11	000010	
195	11	000011	
196	11	000100	
,			Subred Invalida
,			
,			
251	11	111011	
252	11	111100	
253	11	111101	
254	11	111110	
255	11	111111	

Tabla de subneteo.

Realice los siguientes ejercicios.

1. Una compañía tiene la siguiente red: 215.80.40.__
   Se requieren tres subredes y tres equipos por red (como mínimo).
   Realice subneteo y obtenga su tabla.
   a. Discútanse los resultados y elíjase una opción.

Ahora impleméntelo de forma tangible en el laboratorio.
   b. Cree tres equipos de trabajo en el laboratorio.
   c. Realice un ping a un host de otro equipo de trabajo
   ¿Se obtuvo respuesta? _____
   ¿Por qué? _____

Con los conocimientos adquiridos en la practica 2, configure los parámetros necesarios en las terminales de cada equipo, respecto a la opción que se eligió.
   d. Realice nuevamente un ping a un host de otra subred.
   ¿Se obtuvo respuesta? _____
   ¿Por qué? _____

Ahora soliciten al instructor que instale un gateway configurado en la red.
   e. Realice nuevamente el ping.
   ¿Se obtuvo respuesta? _____
   ¿Por qué? _____

2. Teniendo la siguiente Dirección IP: 164.100.221.__
   Obtenga 8 subredes y 16 equipos por subred. (Como mínimo)
   Realice subneteo y obtenga su tabla.

3. Teniendo la dirección IP: 123.1.1.__
   Realice subneteo y obtenga su tabla correspondiente tomando 4 bits para subred.

Evaluación.

1. Dadas las siguientes direcciones y sus mascaras, mencione cuantas subredes y cuantos equipos tiene cada una.

Nota: Tome el tiempo de realización, si excede de 5 min. Solicite a su instructor le aclare sus dudas.

Dir. IP	75.40.200.30		
Mascara	255.255.0.0	subredes: 2 — = _____	Equipos: 2 — = _____
Dir. IP	215.70.80.100		
Mascara	255.255.255.192	subredes: 2 — = _____	Equipos: 2 — = _____
Dir. IP	145.80.173.20		
Mascara	255.255.224.0	subredes: 2 — = _____	Equipos: 2 — = _____
Dir. IP	90.150.210.46		
Mascara	255.255.128.0	subredes: 2 — = _____	Equipos: 2 — = _____
Dir. IP	210.100.48.126		
Mascara	255.255.255.240	subredes: 2 — = _____	Equipos: 2 — = _____
Dir. IP	194.127.35.199		
Mascara	255.255.252.0	subredes: 2 — = _____	Equipos: 2 — = _____

2. Explique la importancia de las mascaras de red y subred.

_____
_____
_____

3. ¿Se pueden crear subredes quitando un sólo bit a la parte de host? ¿Por qué?

_____
_____
_____

También en Internet se pueden realizar ejercicios de subneteo, en la dirección: http://www.nic.unam.mx/herramientas/instrucciones.html

Conclusiones

Que el alumno describa una breve conclusión a la que haya llegado acerca del uso y desarrollo del subneteo.

PRÁCTICA 3- CONFIGURACIÓN DEL PROTOCOLO TCP/IP
(Duración estimada: 60 minutos)

OBJETIVOS

- Que el alumno aprenda a configurar el protocolo de de comunicación TCP/IP.

+ Bajo ambiente gráfico.

- Que el alumno realice pruebas para verificar que el equipo haya sido configurado correctamente.
- Que el alumno realice pruebas para comprobar que el equipo esta en buen estado y funcionando correctamente.

CUESTIONARIO PRELIMINAR

1. Explique brevemente los orígenes del protocolo de comunicación TCP/IP.
2. ¿Qué es la conmutación de paquetes?
3. ¿Qué es un paquete de información?
4. ¿Qué es un gateway?
5. ¿Qué son y para qué sirven las tablas de ruteo?
6. ¿A qué hace referencia el Loopback?
7. ¿Cuál es la dirección que identifica al gateway default y al loopback?
8. ¿Cuáles son las direcciones de equipo reservadas?
9. ¿Qué es y cómo funciona el algoritmo de encaminamiento?
10. ¿Qué es el direccionamiento físico y el direccionamiento lógico?
11. Define dirección estática y dirección dinámica.
12. Concepto de subred.

MARCO TEÓRICO

El protocolo de comunicaciones TCP/IP tiene sus orígenes en el proyecto de la agencia ARPA del gobierno de EUA para construir una red que funcionase con la tecnología de conmutación de paquetes allá por lo años 65, conocida como ARPAnet. Aparte de crear los dispositivos que permitieran la comunicación, se tenía que diseñar un protocolo que hiciera posible el intercambio de paquetes entre los equipos. Ello dio origen al primer protocolo utilizado de comunicación utilizado en ARPAnet, llamado NCP o Protocolo de Control de Red terminado para diciembre de 1970. Este protocolo no duró mucho, ya que tendía a actuar como un controlador de dispositivos y no como un conmutador de paquetes; por lo que en 1973 se empezó a desarrollar un nuevo protocolo denominado TCP (Protocolo de Control de Transmisión). Posteriormente sufrió modificaciones y dividió sus funciones en dos protocolos: TCP, encargado de las funciones de transporte, control de flujo y recuperación de paquetes, y el IP (Protocolo de Internet) encargado del direccionamiento de paquetes.

Posteriormente se incrementaría el protocolo ICMP para control de mensajes y retroalimentación de problemas., el protocolo UDP que brinda un acceso a IP para

aquellas aplicaciones que no requieran de los servicios de TCP, así como una gran variedad más de protocolos de aplicación (HTTP, FTP, Telnet, SMTP, etc.) y administración (SNMP, etc.) que enriquecen los servicios brindados. Es por ello que TCP/IP engloba a una gran cantidad de protocolos y no sólo TCP e IP.

Conmutación de paquetes

La red ARPAnet, y por ende Internet, opera bajo la tecnología de conmutación de paquetes; la cual consiste básicamente en lo siguiente: en un ambiente de redes, conocido comúnmente como *Internet* , que consiste de diversas redes que están enlazadas entre sí para formar una red más grande, se emplean dispositivos especiales que tiene la función de conmutar paquetes de una red a otra, de tal manera que puedan viajar de un equipo fuente a un equipo destino ubicado en otra red. Cuando un equipo tiene que enviar información a la red lo hace a través de paquetes; es decir, que la información a transmitir es dividida en pequeños pedacitos y a cada uno de estos se le añade información suficiente para que pueda viajar de forma independiente por las redes y llegar a su destino; a esto se le llama paquete.

Ruteo

Los dispositivos especiales que realizan la función como la conmutación de paquetes de red en red son los **ruteadores**, los cuales, tiene protocolos que les permiten generar diagramas completos de la estructura que tiene la red. Estos diagramas están en forma de tablas, conocidas como tablas de ruteo; estas, son consultadas por le protocolo IP que debe estar corriendo dentro del ruteador (en el caso de TCP/IP) para tomas las decisiones de cuál es el siguiente punto al que tiene que ser enviado un paquete para que llegue a su destino; es decir, que IP es el encargado de rutear los paquetes; por lo que el ruteo consiste en tomar las decisiones de cuál de todos los caminos posibles, es el que debe seguir un paquete para llegar a su destino, y una vez tomada la decisión, el paquete es liberado o enviado o enviado por dicho camino.

En la práctica, para unir las redes suelen ser empleados **Gateways**, los cuales, a demás de poder desempeñar las funciones de un ruteador, también puede cambiar de protocolos si es necesario.

En el caso de cualquier otro equipo (que no cuente con protocolos de ruteo), la tabla de ruteo se genera automáticamente al encender el equipo a través de la información que ha sido configurada cuando se instaló y configuró el protocolo TCP/IP, y se mantiene fija y sin ningún cambio durante su operación; a menos que se utilicen comando para modificarla manualmente por el usuario. Comparando las tablas de ruteo de los equipos contra las de los ruteadores, las primeras son generalmente más sencillas.

Las tablas de ruteo contienen entre otras cosas dentro de cada entrada, la dirección de una posible red destino y la dirección del ruteador (o gateway) al que tiene que ser enviado el paquete para que llegue a su destino.

Loopback es un nombre ya reconocido por los equipos e identifica al mismo equipo; es decir, que cuando se envía una señal al loopback el mensaje desciende por toda la pila de protocolos, y cuando IP detecta que el mensaje es para el loopback, lo envía de regreso ascendiendo nuevamente por la pila de protocolos hasta la aplicación. De ello se deduce que la señal nunca sale a la red; por lo que se utiliza para probar si el protocolo y demás dispositivos del equipo están funcionando correctamente (aunque el equipo no esté conectado a la red). En algunos sistemas, al *Loopback* suelen darle el nombre de "*Localhost*".

En términos generales, cuando un equipo desea enviar un paquete a un equipo destino se realiza un proceso conocido como "**algoritmo de encaminamiento**".

Direccionamiento

El direccionamiento permite localizar un objeto dentro de un grupo; para lo cual, se asigna una dirección única a cada objeto. En redes podemos clasificar el direccionamiento como: Físico y Lógico.

- El Direccionamiento Físico deriva su nombre del hecho de que estas direcciones son utilizadas en las capas inferiores del modelo OSI: Física y Enlace. Y por otro lado, porque a cada tarjeta d red que es construida, se le asigna una dirección única que es grabada en un circuito dentro de la tarjeta. Existe un organismo internacional encargado de administrar el banco d direcciones disponibles, y cada fabricante de tarjetas de red acude a ellos para solicitar que les sea asignado un banco de direcciones, para que ellos lo administren y puedan incorporar a cada tarjeta que construyen, una dirección de este tipo. Este mecanismo garantiza que dos tarjetas de red, independientemente de quien las fabrique, no tenga la misma dirección.
  A estas direcciones se les llama comúnmente "Direcciones Físicas" o "Direcciones MAC". Un ejemplo de dirección física es: 00-01-02-C9-8B-74.
  Una computadora tendrá una dirección física por cada tarjeta de red que posea.

- El Direccionamiento Lógico es empleado por el direccionamiento que se implementa a través de software; en el caso del direccionamiento numérico empleado por el protocolo IP, o el direccionamiento por nombres empleado por el protocolo DNS; ambos utilizados por TCP/IP en Internet.

  - ✓ Para el caso de IP se utilizan direcciones numéricas conocidas como "Direcciones IP". Estas se componen de 4 bytes que son representados en forma decimal, aislando cada byte por un punto; por ejemplo: 132.248.173.148. Una dirección IP permite identificar dentro de una gran red, como lo es la Internet, a cada equipo dentro de cada una de las redes que la conforman.
    Por otro lado, ya que TCP/IP es el protocolo oficial en Internet, se tiene que llevar un control sobre asignación de direcciones a los equipos u evitar que se dupliquen direcciones. Existe una organización que lleva el control

de las direcciones, y cuando una empresa desea conectarse a Internet, la organización le asigna un bloque de direcciones de a cuerdo a su tamaño. La empresa tiene la responsabilidad de asignar las direcciones IP a cada uno de sus equipos; siempre vigilando que no se repitan.

- ✓ El direccionamiento lógico es el de "nombres", como el empleado por el protocolo DNS (Domain Name System), que a continuación se describe:

  Una dirección por nombres está compuesta por varios nombres separados por un punto; por ejemplo: www.unam.mx

  Este tipo de direcciones surge por necesidad; ya que anteriormente se tenía que identificar a cada computadora en Internet por su dirección IP; lo cual, para nosotros los humanos resultaba u poco complicado al tener que recordar tantos números. Es por esa razón que surge este nuevo direccionamiento en Internet, por ejemplo: la UNAM, que es una institución mexicana, tiene un equipo que utiliza para darle el servicio de web a la comunidad universitaria y al público en general. A dicho equipo se le ha asignado el nombre de www.unam.mx, que es muy fácil de recordar en lugar de su dirección IP 132.248.10.7. el nombre completo del euipo está compuesto por el nombre del equipo (www) más el nombre del dominio al cual pertenece (unam.mx). El nombre del dominio puede estar compuesto por uno o más nombres de dominio; como en este caso, en el cual el dominio de la UNAM pertenece al dominio de mx (México). Otro ejemplo sería www.aragon.unam.mx indicando que el equipo www (servidor de web) pertenece al dominio de aragon (ENEP Aragón) el cual a su vez pertenece al dominio de la unam (UNAM) y este a su vez al dominio de mx (México).
  Al direccionamiento por nombres en esta modalidad se le conoce como direccionamiento por "nombres de dominio" y se implementa a través del protocolo de aplicación de TCP/IP llamado DNS. Básicamente DNS es una base de datos distribuida, a través e la cual, se puede hacer la conversión de direcciones IP a direcciones por nombres o viceversa. Cuando se utiliza este tipo de direccionamiento debe estar al alcance de cualquier equipo.
  Una persona puede asignar cualquier nombre a su computadora; pero si se requiere que ésta sea conocida a nivel mundial, dentro de la comunidad de Internet, el nombre del equipo debe ser registrado dentro de algún dominio, siguiendo los procedimientos establecidos y dentro de los cuales, se verifica que dicho nombre no se repita dentro del dominio. Una vez hecho esto, el nombre de la computadora estará compuesto por su nombre más el nombre del dominio en el cual fue registrado, separado por un punto.

Cuando se desea conectar una nueva computadora a una red, se le tiene que instalar el protocolo de comunicación al equipo y después configurarlo. En el caso de TCP/IP, para

configurarlo se tienen que dar diversos parámetros y entre ellos se encuentran las direcciones lógicas. Estos suelen ser asignados a los equipos de alguna de las dos siguientes formas:

- ✓ *De forma manual* dando estos parámetros durante el proceso de configuración, por lo que estos datos quedaran almacenados en algún archivo dentro del equipo. De esta forma, cada vez que equipo se encienda y arranque el software. Éste se configurará quedando siempre con los mismos datos; y entre ellos, la dirección lógica; que en el caso del Protocolo IP, es una dirección IP. Este parámetro no cambiará hasta que el usuario modifique y grabe los cambios en los archivos de configuración. A las direcciones lógicas que son asignadas de esta forma se les llama **direcciones estáticas.**

- ✓ *De forma automática.* en esta modalidad deberá existir algún mecanismo para que el equipo adquiera sus parámetros, y su dirección, de alguna forma automática. En el caso de TCP/IP nuevamente, se emplea el protocolo de aplicación llamado "DHCP". En este sistema, deberá existir en la red local donde se encuentra conectado el equipo, un servidor DHCP; el cual asigna de forma dinámica algunos parámetros a los equipos que lo soliciten (dirección IP, mascara de subred, etc.).

- ✓ Cuando un equipo se enciende, revisa sus archivos de configuración para establecer sus parámetros de funcionamiento; si se establece que debe obtenerlos automáticamente de la red, se utilizará el protocolo DHCP para enviar una señal al servidor DHCP solicitándoselos. Cuando el servidor recibe la petición, regresa una respuesta al equipo en la que se incluyen los parámetros, que han sido tomados de una base de datos que el servidor posee.

- ✓ El servidor DHCP lleva un control de los equipos que le han solicitado parámetros, así como la hora en que les han otorgado *(permiso obtenido)* y hasta cuando podrán ser usados *(permiso caduca).*

- ✓ Cuando un permiso alcanza el tiempo establecido para poder utilizar estos valores *(permiso caduca)*, de manera automática envía una señal al servidor DHCP para pedir una renovación de tiempo, otorgándole un nuevo límite, hasta el cual, se podrán seguir utilizando los valores. Cuando el equipo es apagado, y por ,o tanto no renueva su tiepo, el servidor DHCP está en la posibilidad de asignar estos valores a otro equipo; es por ello que cada que se encienda el equipo, éste puede tener distintos valores. A este tipo de direcciones se les conoce como **direcciones dinámicas**; y nunca deben ser asignadas a equipos que fungirán como servidores.

HERRAMIENTAS Y RECURSOS

- 1 Equipo de cómputo con sistema operativo Windows 98 por cada grupo de trabajo.
- Conexión a Internet.
- Se pide al alumno los conocimientos suficientes para manejar S.O. Windows 98.
- Haber contestado el cuestionario preliminar.
  * El material se encuentra en el laboratorio.

DESARROLLO

Explicación: el alumno llevará un registro (donde se le indique) de los eventos que se vayan desarrollando para posteriormente entregar un reporte con los siguientes criterios:

- Los pasos de mayor grado de dificultad al realizar la práctica.
- Problemas encontrados al realizar la práctica.
- Observaciones
- Resultados obtenidos al realizar las pruebas.
- Respuestas a las preguntas que se realicen a lo largo de la práctica.

PARTE DE CONFIGURACIÓN DEL PROTOCOLO TCP/IP

Paso 1. Encienda el equipo que le haya sido asignado.

Paso 2. Cuando aparezca la ventana de *"Contraseña de Red"*, accese al ambiente Windows digitando en *"Nombre de Usuario"* el nombre de la PC y en el de *"Contraseña"* vuelva a escribir el nombre de la PC. Por ultimo de un clic en botón de *"Aceptar"* o presione la tecla de *"Enter"*.

Paso 3. Existe una herramienta en el escritorio llamada *"Entorno de Red"*, colocando el puntero del Mouse sobre el icono de la herramienta de un clic con el botón secundario del Mouse y seleccione la opción *"Propiedades"* como lo muestra la Figura 1.

Paso 4. Será desplegada la ventana de *"Red"*.

Paso 5. Existen varias opciones dentro de la ventana de *"Red"* seleccione la pestaña de *"Configuración"*. A continuación, en la parte de *"Están instalados los siguientes componentes de red"* seleccione el protocolo *"TCP/IP"* que es asignado a su tarjeta de red y posteriormente presione el botón de *"Propiedades"*.

Paso 6. La ventana que aparece se refiere a las *"Propiedades de TCP/IP"* y a través de ésta se pueden configurar todos los parámetros necesarios para que este protocolo funcione. A continuación seleccione la pestaña de *"Dirección IP"*.

Dirección IP y *Mascara de Subred* son parámetros que se pueden configurar siempre y cuando la opción *"Especificar una dirección IP"* e introduzca la Dirección IP y Mascara de Subred que su instructor le indique.

Paso 7. Mencione ¿Cuál es el mecanismo que utiliza la opción *"Obtener una dirección IP automáticamente"*?_____
_____.

Paso 8. Seleccione la pestaña *"Puerta de enlace"*. En el cuadro de *"Puertas de enlace instaladas"* aparecen listados los distintos gateway que se pueden utilizar para conectarse a otras redes. En este caso no se han sido configurados aún.
A continuación agregue la puerta de enlace que le sea indicado por el instructor en el cuadro *"Nueva puerta de enlace"* y en seguida presione el botón *"Agregar"*. Si el botón no es presionado la operación no se efectuará y por lo tanto no se podrá utilizar.

Paso 9. Seleccione la pestaña de *"Configuración de DNS"*.
Esta ventana permite utilizar un servidor DNS para la resolución de nombres. Active la opción *"Activar DNS"* con el fin de que se activen los campos de configuración inferiores.
Introduzca los datos que le proporcione su instructor en los campos de *"Host"* y *"Dominio"*.
Establezca la dirección IP del servidor DNS que su instructor le indique en el primer cuadro de captura del campo *"Orden de búsqueda del servidor DNS"* y posteriormente presione el botón de *"Agregar"* para que sea agregado a la lista, de lo contrario no entrará en función.

Al especificar más de un servidor DNS, cuando se deba resolver un nombre utilizará el primero, si éste no está funcionando o no lo puede resolver, se buscará en el segundo y así sucesivamente.

Explicación: Las demás pestañas permiten establecer parámetros adicionales y no serán tratados en ésta práctica.

Paso 10. De un clic en el botón de *"Aceptar"* para que los cambios sean guardados, cierre la ventana de *"Propiedades d TCP/IP"*.

Paso 11. De un clic nuevamente en el botón de *"Aceptar"* para cerrar la ventana de *"Red"*.

Paso 12. Se abrirá una ventana de *"Cambios de configuración del sistema"* preguntando si desea reiniciar el equipo para que los cambios tengan efecto, para ello presione el botón *"Si"*.

Paso 13. Una vez que arranque el equipo entre a sesión nuevamente.

PARTE DE COMPROBACIÓN DE LA CONFIGURACIÓN

Paso 14. Para comprobar que el equipo se encuentra configurado correctamente y tiene acceso a la red, ejecute una ventana del *"Internet Explorer"* y en el campo de *"dirección"* escriba *"http://www.unam.mx* . Al realizar este paso debe establecerse conexión con el servidor web de la UNAM y se deberá desplegar su página en la pantalla. De lo contrario pida apoyo a su asesor para localizar la falla. Si se desplegó la pagina, cierre la ventana del *"Internet Explorer"* y siga con el siguiente paso de la práctica.

Paso 15. Abra una ventana de *"MS-DOS"* dando clic en el menú *"Inicio"* y seleccionando la opción *"Ejecutar"* a continuación escriba *command* en el campo y por ultimo de un clic en el botón de *"Aceptar"* o presione tecla de *"Enter"*.

Paso 16. En el prompt de *"MS-DOS"* ejecute el comando:
C:\WINDOWS>IPCONFIG

Paso 17. Anote los parámetros que correspondan a su tarjeta de red de:

Dirección IP: _____
Máscara de Subred: _____
Puerta de enlace predeterminada: _____

Paso 18. En el prompt de *"MS-DOS"* ejecute el comando:
C:\WINDOWS>IPCONFIG /all | more

Como se puede observar, en la pantalla sale información que se encuentra dividida en dos partes: *"Configuración IP de Windows 98"* y *"0 Ethernet adaptador"*. De la primera, los parámetros que nos interesan para esta práctica son, el *"Nombre del Host"*, y el *"Servidor de DNS"*, en el cual se establece la dirección numérica del equipo servidor DNS.

En la segunda parte *"0 Ethernet adaptador"*, los parámetros que nos interesan son: la *"Dirección Física"*, que se refiere a la dirección que tiene grabada físicamente la tarjeta de red 0, para este caso. El de *"DHCP activado"*, que básicamente indica si este protocolo se encuentra activado y que al estarlo los parámetros se asignaran de forma dinámica.; así como los parámetros de *"Permiso obtenido"* y *"Permiso caduca"*, que se encargan de establecer la vigencia del derecho a usarlos. Los de *"Servidor WINS primario"* y *"Servidor WINS secundario"*, que se encargan de determinar si es que se esta utilizando un servidor WINS que se encuentre dentro de la red local, en último lugar, los parámetros de *"Dirección IP"*, *"Mascara de red"* y *"Puerta de Enlace Predeterminada"*, que deben coincidir con los datos obtenidos en el paso 17 y por supuesto con los que fueron asignados por el asesor.

Anote cada uno de los parámetros establecidos en este punto.

_____

_____

Paso 19. De los conocimientos adquiridos en el paso anterior conteste las siguientes preguntas:

- ✓ ¿De qué forma se encuentra establecida la dirección IP del equipo?
- ✓ ¿A qué dominio pertenece su equipo?
- ✓ ¿Se encuentra activado algún servidor WINS?
- ✓ El parámetro de "*permiso caduca*" ¿tiene algún valor establecido?
- ✓ En caso negativo, ¿qué significa eso?
- ✓ ¿Qué función tiene la opción "Obtener una dirección IP automáticamente?

Nota: Todos los datos obtenido en el paso17 tienen que coincidir con los datos que su asesor le proporciono para configurar su equipo con el protocolo TCP/IP, si es así paso al paso siguiente de lo contrario pregunte a su asesor y verifiquen la posible falla.

CONCLUSIONES

Que el alumno haga un análisis de cada uno de los pasos que llevo a cabo y comente dudas y haga aclaraciones de todo lo que pudo aprender en esta práctica.

PRÁCTICA 4 – MANEJO DE UN ANALIZADOR DE PROTOCOLOS (ETHEREAL)
(Duración estimada: 60 minutos)

OBJETIVOS

- Que el alumno observe y analice el comportamiento de protocolos.
- Que alumnos aprenda a utilizar una herramienta capaz de monitorear el tráfico en la red.
- Que el alumno aprenda a revisar los paquetes de datos en una red activa como desde un archivo de captura previamente generado.

CUESTIONARIO PRELIMINAR

1. ¿Qué es un protocolo?
2. ¿Qué es un analizador de protocolos?
3. ¿Qué es un sniffer?
4. ¿Qué es Ethereal?
5. ¿Para qué sirve Ethereal?
6. ¿Qué plataformas soportan a este software?
7. ¿Qué es un filtro de captura?
8. ¿Qué es un filtro de despliegue?
9. ¿Qué es una interfaz gráfica?

MARCO TEÓRICO

Analizadores de Protocolos de Red.

Para observar y analizar el comportamiento de los protocolos de red es preciso disponer de una herramienta capaz de monitorear el tráfico en la red y mostrarlo en una forma legible. Las herramientas que capturan y muestran el tráfico existente en una interfaz de red se denominan analizadores de protocolos de red, analizadores de paquetes, "packet sniffers" o simplemente "sniffers" (del inglés sniff, olfatear). Para visualizar el tráfico los analizadores de protocolo colocan la tarjeta de red en modo promiscuo, una modalidad en

la cual es capturado todo el tráfico visible para la tarjeta de red. En una red Ethernet una interfaz de red en modo promiscuo puede ver todo el tráfico generado por todos los equipos que comparten el mismo conjunto de cables y concentradores (hubs). El modo promiscuo implica riesgos evidentes de seguridad, por lo que su uso suele limitarse al supervisor.

Ethereal.

Ethereal es un analizador de protocolos con interfaz gráfica capaz de reconocer muchos protocolos distintos. Permite tanto revisar los paquetes de datos en una red activa como desde un archivo de captura previamente generado; es capaz de comprender diversos formatos de archivo propios de otros programas de captura, en particular el clásico tcpdump.

Uso de Ethereal.

El programa Ethereal puede hacerse a través del menú de invocación del ambiente gráfico Windows o desde una terminal Unix si no existe la opción en el menú. Si se hace a través de una terminal Unix, el comando

ethereal &

Arranca el programa y devuelve el control de la terminal al usuario para poder continuar ingresando comandos. El símbolo & arranca el programa como proceso independiente de la terminal.

En la presente práctica se ejecutara este programa bajo sistema operativo Windows 98. La figura muestra la ventana principal de Ethereal luego de una captura de datos. Inicialmente, esta ventana aparece vacía.

En la ventana principal de Ethereal se reconocen tres áreas de despliegue (Figura 1):

Resumen de paquetes capturados, un paquete por línea; uno de ellos ha sido seleccionado como paquete actual (dando clic sobre la línea del paquete). Al desplazarse en la lista y cambiar el paquete actual se actualizan las otras dos ventanas, donde se despliega en dos formatos diferentes el contenido del paquete.

Detalles de encabezado de protocolos para el paquete seleccionado; los encabezados pueden abrirse (clic en +) para ver mayor detalle, o cerrarse (clic en -) para ocupar sólo una línea.

Datos crudos del paquete, representación hexadecimal y ASCII del encabezado del paquete seleccionado en el campo del medio.

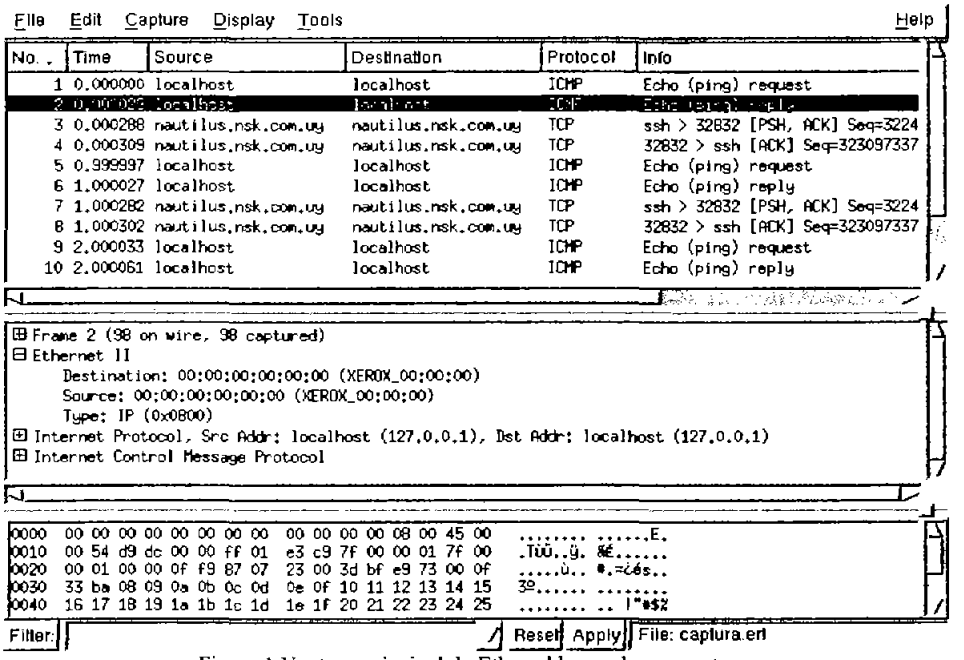


Figura.1.Ventana principal de Ethereal luego de una captura.

Para iniciar la captura de datos, elegir las opciones de menú Capture: Start (Capturar, Comienzo). En la ventana de opciones de captura (ver figura), debe fijarse al menos la interfaz sobre la que se quiere realizar la captura. Los nombres varían según los sistemas operativos; la interfaz lo (loopback) permite enviar y recibir paquetes en la propia máquina (Figura 2).

Para capturar en un archivo debe indicarse su nombre en el cuadro "Capture file(s)" de la ventana de Opciones de Captura (Capture: Start abre esta ventana). Estos archivos pueden ser examinados luego con el propio Ethereal mediante la opción de menú File: Open. El tráfico ya capturado puede grabarse en un archivo eligiendo File: Print (Archivo: Imprimir); esta opción graba en formato legible (texto).

La ventana de estado (Figura 3) muestra en tiempo real la cantidad de paquetes capturados, en total y de algunos tipos corrientes. La situación de captura se mantiene hasta que se presiona el botón Stop. Luego de unos instantes aparecen los paquetes capturados, tal cual se ve en la imagen de la ventana principal. Si se activó la opción de actualizar lista de paquetes en tiempo real ("Update list of packets in real time") estos se visualizan a medida que son capturados.

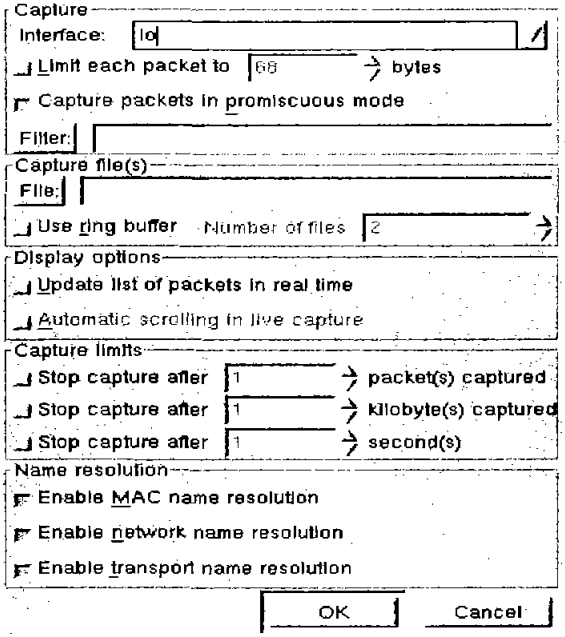


Figura 2.Opciones de captura.

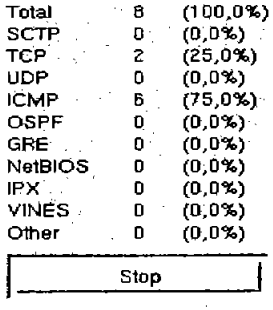


Figura 3. Estado de captura.

Ayuda, documentación.

La ventana de ayuda (Figura 4) da una reseña del programa (Overview), lista los protocolos reconocidos, lista los nombres de los filtros posibles (Display filters) y refiere a la página man de tcpdump para la sintaxis de filtros de captura (Capture filters); la sintaxis de filtrado en la captura es diferente de la sintaxis de filtrado en el despliegue.

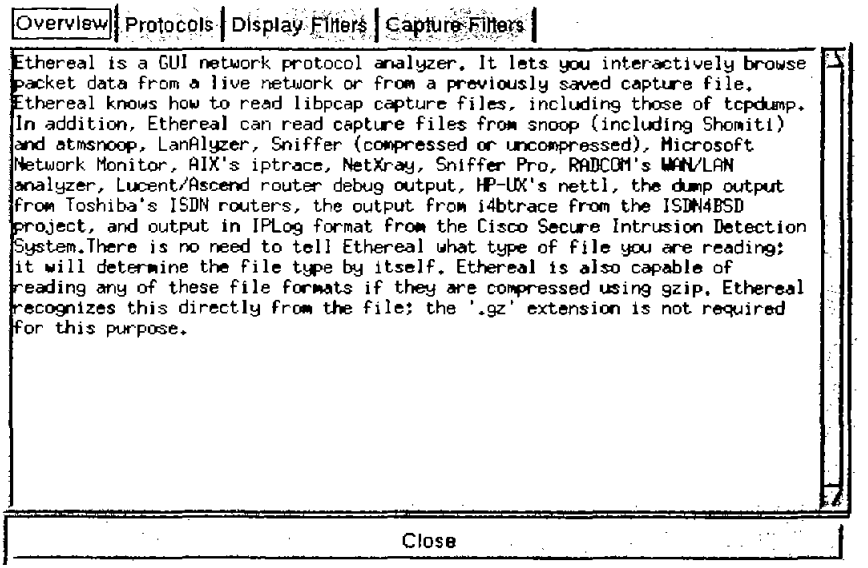


Figura 4. Ayuda y Documentación

Filtrado de paquetes.

El filtrado de paquetes permite capturar o desplegar sólo aquellos paquetes de interés para el estudio en curso, desconociendo la existencia de otros. Ethereal tiene dos modos de filtro distintos:

Filtro de captura: sólo se retienen los paquetes que cumplen la expresión filtro. Define lo que se guarda (Figura 5).
Filtro de despliegue: de los paquetes capturados, sólo se muestran los paquetes que cumplen la expresión filtro (Figura 6). Define lo que se ve de lo que hay guardado.

La sintaxis de escritura de ambos tipos de filtro es diferente. Los filtros de captura siguen la sintaxis del comando tcpdump y deben ser escritos en el cuadro Filter de la ventana de opciones de captura, antes de iniciar la captura. Los filtros de despliegue se fijan en el cuadro File de la ventana principal de Ethereal. En ambos casos, presionando este botón File aparece un cuadro de diálogo que permite asignar un nombre a la expresión filtro construida.

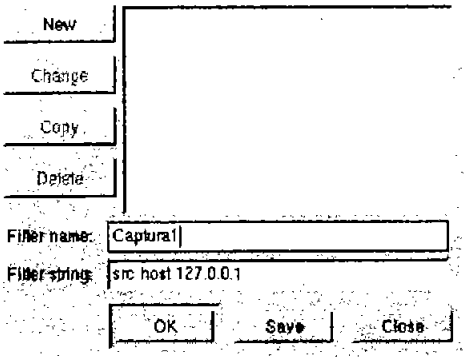


Figura 5. Diálogo para construir filtro de captura

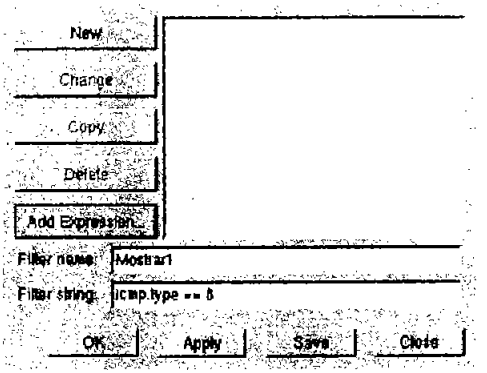


Figura 6. Diálogo para construir filtro de despliegue.

Para los filtros de despliegue existe una ayuda adicional en el botón Add Expression, que permite construir la expresión eligiendo el protocolo, sus campos y operadores relaciónales (Figura 7).

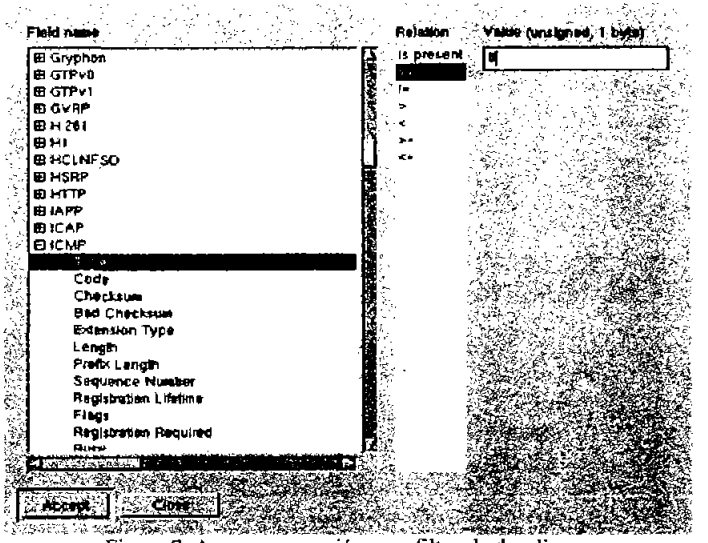


Figura 7. Agregar expresión para filtro de despliegue

HERRAMIENTAS Y RECURSOS

-1 equipo de cómputo por grupo de trabajo con Sistema Operativo Windows 98 y el software de Ethereal previamente instalado.
-Conexión a Internet
-Se pide a los alumnos los conocimientos suficientes para manejar S.O. Windows 98.
-Haber contestado el cuestionario preliminar.
*El material se encuentra en el laboratorio.

DESARROLLO

Paso 1. Encienda el equipo que le haya sido asignado.

Paso 2. Cuando aparezca la ventana de *"Contraseña de Red"*, accese al ambiente Windows digitando en *"Nombre de Usuario"*el nombre de la PC y en el de *"Contraseña"* vuelva a escribir el nombre de la PC. Por ultimo de un clic en el botón de *"Aceptar"* o presione la tecla de *"Enter"*.

Ejercicio 1: Captura, reconocimiento, grabar como texto, grabar en formato Ethereal, visualizar.

Paso 3. Iniciar una captura (Capture: Start), elegir la interfaz lo. Arrancar la captura presionando el botón OK.

Paso 4. En una ventana aparte, en una terminal de comandos MS-DOS, escribir
ping -c3 localhost.

Aguardar a que termine de ejecutarse el comando.

Paso 5. Terminar la captura (Stop en la ventana de captura de Ethereal).

Paso 6. Examinar la captura. Reconocer los paquetes pedido - respuesta (request - reply) del protocolo ICMP (Internet Control Message Protocol).

Paso 7. Grabar la captura, como texto, en un archivo: File: Print, tic en File, indicar un nombre de archivo (por ejemplo captura1.txt).

Paso 8. Visualizar el archivo; verificar que es legible.

Paso 9. Grabar la captura en el formato propio de Ethereal: File: Save as...; indicar un nombre de archivo (por ejemplo captura1.ether). Este archivo no es legible como texto, debe ser visualizado con Ethereal o con tcpdump.

Paso 10. Visualizar el archivo de captura en formato Ethereal: File, Open, elegir el archivo. Verificar que se visualiza correctamente.

Nota: Si se desea examinar los paquetes a medida que van siendo capturados, activar en la ventana de Opciones de Captura "Update list of packets in real time" y "Automatic scrolling in live capture".

Ejercicio 2: Captura, reconocimiento, grabar como texto, grabar en formato Ethereal, visualizar y aplicar un filtro de captura.

Paso 1. Iniciar una captura dando un clic en el menú *"Capture"* y seleccionando *"Start"*.

Paso 2. De un clic en el botón *"New"*. A continuación en el área de *"Properties"* escriba en la parte de *"Filter name"* Captura1 y en la parte de *"Filter string"* src host 132.248.173.172

Paso 3. En una ventana aparte, en una terminal de comandos MS-DOS, escribir
ping 132.248.173.148

Aguardar a que termine de ejecutarse el comando.

Paso 4. Terminar la captura presionando el botón de *"Stop"* en la ventana de captura de Ethereal.

Paso 5. Examinar la captura. Reconocer los paquetes pedidos.

Paso 6. A continuación transcriba los datos obtenidos en la interfaz de la primera ventana.

Paso 7: Elija uno de los datos, analícelo y explique con sus propias palabras el significado de cada uno de los parámetros obtenidos a través de la captura.

No.
Time
Source

Destination
Protocol
Info

Paso 8. Grabar la captura como texto en un archivo. De un clic en el menú "*File*"y a continuación en la opción *"Save As"*, indicar un nombre de archivo (por ejemplo captura1.txt).

Paso 9. Visualizar el archivo; verificar que es legible.

Paso 10. Grabar la captura en el formato propio de Ethereal. De un clic en el menú "*File*" y posteriormente en la opción *"Save As"* indicar un nombre de archivo (por ejemplo captura1.ether). Este archivo no es legible como texto, debe ser visualizado con Ethereal o con tcpdump.

Paso 11. Visualizar el archivo de captura en formato Ethereal. De un clic en el menú "*File*" y posteriormente en la opción *"Open"*, elegir el archivo. Verificar que se visualiza correctamente.

Ejercicio 3: Captura, reconocimiento, grabar como texto, grabar en formato Ethereal, visualizar y aplicar un filtro de despliegue.

Paso 1. Para poner un filtro de despliegue de un clic en el botón *"Expression..."* y a continuación se desplegara un cuadro de dialogo "*Ethereal: Filter expresión"* en la parte de *"Field name"* busque la opción ICMP y de un clic en la flecha que se encuentra a la izquierda del protocolo, del menú que sale elija la opción icmp.type –Type. A continuación en la parte de *"Relation"* de clic en el símbolo de = =, en la parte de *"Value"* escriba el número 8, de un clic en el botón de *"OK"* para guardar la opción del filtro.

Paso 2. Iniciar una captura dando un clic en el menú *"Capture"* y seleccionando *"Start"*.

Paso 3. *"Capture Filter"* a continuación se desplegara la ventana de *"Ethereal: Capture Filter"*.

Paso 4. De un clic en el botón *"New"*. A continuación en el área de *"Properties"* escriba en la parte de *"Filter name"* Captura1 y en la parte de *"Filter string"* src host 132.248.173.172 y dar un clic en el botón *"Ok"*

Paso 5. En una ventana aparte, en una terminal de comandos MS-DOS, escribir
ping 132.248.173.148

Aguardar a que termine de ejecutarse el comando.

Paso 6. Terminar la captura presionando el botón de "*Stop*" en la ventana de captura de Ethereal.

Paso 7. Examinar la captura. Reconocer los paquetes pedidos.

Paso 8. A continuación transcriba los datos obtenidos en la interfaz de la primer ventana.

Paso 9: Elija uno de los datos, analícelo y explique con sus propias palabras el significado de cada uno de los parámetros obtenidos a través de la captura.

No.
Time
Source
Destination
Protocol
Info

Paso 10. Grabar la captura como texto en un archivo. De un clic en el menú "*File*"y a continuación en la opción "*Save As*", indicar un nombre de archivo (por ejemplo captura1.txt).

Paso 11. Visualizar el archivo; verificar que es legible.

Paso 12. Grabar la captura en el formato propio de Ethereal. De un clic en el menú "*File*" y posteriormente en la opción "*Save As*" indicar un nombre de archivo (por ejemplo captura1.ether). Este archivo no es legible como texto, debe ser visualizado con Ethereal o con tcpdump.

Paso 13. Visualizar el archivo de captura en formato Ethereal. De un clic en el menú "*File*" y posteriormente en la opción "*Open*", elegir el archivo. Verificar que se visualiza correctamente.

Paso 14. De los conocimientos adquiridos durante la práctica conteste las siguientes preguntas:

- ✓ Menciona algunos beneficios que ofrezca el hecho de analizar el comportamiento de los protocolos de una red.

- ✓ ¿Qué utilidad le asignas al hecho de poder revisar los paquetes de datos de una red activa?

- ✓ Describe brevemente los datos capturados en la parte de la ventana principal de Ethereal que pertenecen a la *ventana de encabezado de protocolos para el paquete seleccionado.*

- ✓ ¿Cuál es la diferencia entre un filtro de captura y un filtro de despliegue?

CONCLUSIONES

Que el alumno haga un análisis de cada uno de los pasos que llevo a cabo y comente dudas y haga aclaraciones de todo lo que pudo aprender en esta práctica.

PRÁCTICA 5 – ANÁLISIS DE LOS PROTOCOLOS TCP E ICMP A TRAVÉS DE UN ANALIZADOR DE PROTOCOLOS (ETHEREAL)
(Duración estimada: 90 minutos)

OBJETIVOS

- Que el alumno observe y analice el comportamiento de los protocolos TCP e ICMP.
- Que el alumno aprenda a revisar los paquetes de datos de cada uno de los protocolos mencionados antes.
- Que el alumno aprenda a interpretar la información capturada de cada uno de los protocolos.
- Que el alumno aprenda a través de Ethereal cada una de las partes que componen a dichos protocolos.
- Que el alumno analice la importancia para un administrador de red el hecho de saber analizar un protocolo.

MARCO TEÓRICO

OSI y TCP/IP

La adopción del TCP/IP no está en conflicto con las normas OSI, debido a que los dod se produjeron de manera concurrente. De alguna manera, el TCP/IP contribuyó al OSI y viceversa. Sin embargo, existen varias diferencias importantes, las cuales surgen de los requerimientos básicos del TCP/IP que son:

- Un conjunto común de aplicaciones.
- Enrutamiento dinámico.
- Protocolos sin conexión en el nivel de red.
- Conectividad universal.
- Intercambio de paquetes.

Las diferencias entre la arquitectura OSI y la del TCP/IP se relacionan con las capas encima del nivel de transporte y aquellas del nivel de red. OSI tiene una capa de sesión y una de presentación, en tanto que TCP/IP combina ambas en una capa de aplicación. El requerimiento de un protocolo sin conexión, también requirió que el TCP/IP incluyera a demás, las capas de sesión y presentación del modelo OSI en la capa de aplicación del TCP/IP. En la figura 1 se muestra una vista esquemática de la estructura en capas del TCP/IP, comparada con el modelo de siete capas del OSI.TCP/IP llama subredes a los elementos diferentes del nivel de red.

Modelo OSI	TCP/IP (Internet)
Aplicación	
Presentación	Aplicación
Sesión	
Transporte	
Red	
Vinculación de Datos	
Física	

Figura 1. La estructura en capas del OSI y del TCP/IP.

OSI y TCP/IP no son incompatibles, pero tampoco son compatibles de manera perfecta. Ambos tienen una arquitectura en capas, pero la arquitectura OSI está definida con mucho mayor rigor y las capas son más independientes que las del TCP/IP.

Hubo algo de alboroto acerca de la combinación del nivel de red, aunque pronto fue obvio que el argumento era académico, ya que la mayor pare de las realizaciones del modelo OSI combinaban los niveles físico y de vinculación en un controlador inteligente (como una tarjeta de red). La combinación de las dos capas en una sola tenía un beneficio importante: permitía que se diseñara una subred independiente de cualesquiera protocolos de red, debido a que el TCP/IP no se percataba de los detalles. Esto permitía a las redes patentadas autocotenidas poner en práctica los protocolos TCP/IP para una conectividad fuera de sus sistemas cerrados.
El enfoque en capas dio origen al nombre TCP/IP. La capa de transporte usa el Transmission Control Protocol (TCP) o una de diversas variantes, como el User Datagram Protocol (UDP).Sin embargo, sólo existe un protocolo para el nivel de red: el Internet Protocol (IP). Esto es lo que asegura la conectividad universal del sistema, uno de los objetivos primarios del diseño.

UNIDADES DE DATOS DE PROTOCOLO TCP

El TCP debe comunicarse con el IP en la capa de abajo (usando un método defino por el IP) y con las aplicaciones en la capa superior (usando los primitivos TCP-ULP). El TCP también debe comunicarse con otras implementaciones TCP a través de las redes. Para hacer esto, usa Unidades de Datos de Protocolo (Protocol Data Units, PDU), las cuales se llaman segmentos en el lenguaje TCP.

El diseño de las TCP (por lo común llamada encabezado) se muestran en la Figura 2.

<table>
<tr><td colspan="6">Puerto Fuente (16 bits)</td><td colspan="2">Destino (16 bits)</td></tr>
<tr><td colspan="8">Número de Secuencia (32 bits)</td></tr>
<tr><td colspan="8">Número de acuse de recibo (32 bits)</td></tr>
<tr><td>Compensación de datos (4 bits)</td><td>Reservado (6 bits)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Ventana (16 bits)</td></tr>
<tr><td colspan="6">Suma de verificación (16 bits)</td><td colspan="2">Señalador Urgente (16 bits)</td></tr>
<tr><td colspan="8">Opciones y Relleno</td></tr>
</table>

Figura 2. Encabezado TCP

Los diferentes campos son como siguen:

- *Puerto fuente*: Un campo de 16 bits que identifica al usuario TCP local (por lo general un programa de aplicación de capa superior).
- *Puerto Destino*: Un campo de 16 bits que identifica al usuario TCP de la máquina remota.
- *Número de Secuencia*: Un número que indica la posición del bloque actual en el mensaje total. Este número se usa también entre dos implementaciones TCP para proporcionar el número de secuencia de envío inicial (ISS).
- *Número de acuse de recibo*: Un número que indica el siguiente número de secuencia esperado. De una manera ambigua, éste muestra además el número de secuencia de los últimos datos recibidos; muestra el último número se secuencia recibido más 1.
- *Compensación de datos*: El número de palabras de 32 bits que están en el encabezado TCP. Este campo se usa para identificar el inicio del campo de datos.
- *Reservado*: Un campo de 6 bits reservado para uso futuro. Los bits 6 deben fijarse en 0.
- *Bandera Urg*: Si está activa (un valor de 1), indica que el campo del señalador urgente es significativo.
- *Bandera Ack*: Si esta activa, indica que el campo Acuse de recibo es significativo.
- *Bandera Psh*: Si esta activa, indica que la función push debe ejecutarse.
- *Bandera Syn*: Si está activa, indica que los números de secuencia deben sincronizarse. Esta bandera se usa cuando se está estableciendo una conexión.
- *Bandera Rst*: Si está activa, indica que la conexión debe reiniciarse.
- *Bandera Fin*: Si está activa, indica que el transmisor no tiene más datos que enviar. Éste es el equivalente de un marcador de fin de la transmisión.
- *Ventana*: Un número que indica cuántos bloques de datos puede aceptar la máquina receptora.
- *Suma de verificación*: Calculada tomando el complemento de uno de 16 bits, de la suma de complemento de uno de las palabras de 16 bits en el encabezado (incluyendo seudoencabezado) y texto juntos.
- *Señalador urgente*: Usado si se estableció la bandera urg; indica la parte del mensaje de datos que es urgente al especificar la compensación del número de

secuencia en el encabezado. El TCP no toma ninguna acción específica con respecto a los datos urgentes, la acción la determina la aplicación.

- *Opciones*: Similar al campo Opciones del encabezado IP, éste se usa para especificar opciones del TCP. Cada opción consta de un número de opción (un byte), el número de bytes en ésta y los valores de la opción. En la actualidad, sólo están definidas tres opciones para el TCP:

  0 Fin de la lista de operaciones.
  1 No operación.
  2 Tamaño máximo del segmento.

- *Relleno*: Rellenado para asegurar que el encabezado es un múltiplo de 32 bits.

PUERTOS

Todas las aplicaciones de capa superior que usan el TCP tienen un número de puerto que identifica a la aplicación. En teoría, los números de puerto pueden asignarse en máquinas individuales o en cualquier parte que desee el administrador, pero se han adoptado algunas convenciones para permitir mejores comunicaciones entre las implementaciones TCP. Esto permite al número de puerto identificar el tipo de servicio que le está solicitando un sistema TCP a otro. Los números de puerto pueden cambiarse, aunque esto puede causar dificultades. La mayor parte de los sistemas mantienen un archivo de números de puerto y su correspondiente servicio.

De manera característica, los números de puerto arriba de 255 están reservados para su uso privado de la maquina local, pero los números por debajo de 255 se usan para procesos usados con frecuencia. Una lista de números de puerto usados con frecuencia la publica la Internet Assigned Numbers Authority /Autoridad de Números Asignados de Internet) y está disponible por medio de una RFC o, en muchos sitios que ofrecen archivos de resumen Internet para su transferencia. Por lo común, los números de puerto usados en esta lista se muestran en la Tabla 1. los números 0 y 255 están reservados.

TCP Y CONEXIONES

El TCP tiene muchas reglas impuestas de la manera como comunica. Estas reglas y los procesos que sigue el TCP para establecer una conexión, transferir datos y terminar una conexión, por lo general se presentan en diagramas de estado. (Debido a que el TCP es un protocolo controlado por el estado, sus acciones dependen del estado de una bandera o creación parecida). Es difícil evitar los diagramas de estado demasiado complejos, de modo que pueden usarse diagramas de flujo como un método útil para entender al TCP.

ESTABLECIEMIENTO DE UNA CONEXIÓN

Puede establecerse una conexión entre dos máquinas sólo si existe una conexión entre los dos sockets, ambas máquinas están de acuerdo en la conexión y ambas máquinas tienen recursos TCP adecuados, para servir a la conexión. Si no se cumple cualquiera de estas condiciones, no puede hacerse la conexión. La aceptación de conexiones la puede desencadenar una aplicación o una rutina de administración de sistema.

Cuando se establece una conexión se le dan ciertas propiedades que son válidas hasta que la conexión se cierra. De manera común, éstas son un valor de precedencia y un valor de seguridad. Estos parámetros los acuerdan las dos aplicaciones cuando la conexión está en el proceso de establecerse.

En la mayoría de los casos, una conexión la esperan dos aplicaciones, así que emiten solicitudes abiertas ya sea activas o pasivas. La figura 3 muestra un diagrama de flujo para un TCP abierto. El proceso comienza con el TCP de la Maquina A, que recibe una solicitud para una conexión de su ULP, para lo cual envía un primitivo abierto activo a la Maquina B. El segmento que se crea tiene activada la bandera Syn y tiene asignado un número de secuencia. El diagrama muestra esto con la notación Syn SEQ 50, indicando que la bandera SYN está activada y que el número de secuencia (Initial Send Séquense, ISS) es 50. (Podría haberse elegido cualquier número).

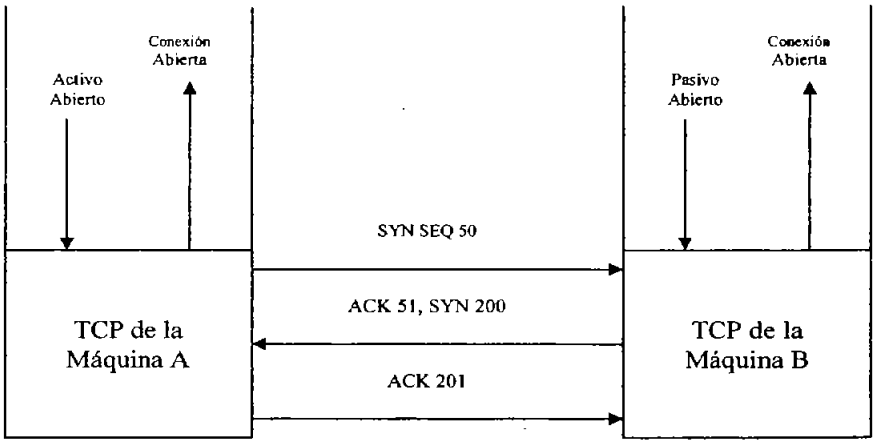


Figura 3. Establecimiento de una conexión

La aplicación en la Máquina B ha enviado una instrucción pasiva abierta a su TCP. Cuando se recibe el segmento SYN SEQ 50, el TCP de la Maquina 50, el TCP de la máquina B envía de regreso un acuse de recibo a la Máquina A, con el número de secuencia de 51. la Máquina B también establece por su cuenta un numero ISS. El diagrama muestra este mensaje como "ACK 51; SYN200", lo que indica que el mensaje es un acuse de recibo con el número de secuencia 51, tiene la bandera Syn activada y tiene u ISS de 200.

Tras la recepción, la Máquina A envía de vuelta su propio mensaje de acuse de recibo con el número de secuencia establecido en 201. Esto es "ACK 201" en el diagrama. Luego, habiendo abierto y acusado recibo de la conexión, la Máquina A y la Máquina B envían mensajes de conexión abierta a través del ULP a las aplicaciones solicitantes.

No es necesario que la máquina remota tenga una instrucción pasiva abierta. En este caso, la máquina transmisora proporciona tanto el número de socket transmisor con el número de socket receptor, al igual que los valores de precedencia, seguridad y tiempo agotado. Es común que las dos aplicaciones soliciten un activo abierto al mismo tiempo. Esto se resuelve con bastante facilidad, aunque implica un poco más de tráfico en la red.

El servicio de transporte de datos TCP en realidad incluye seis subservicios:

- **Dúplex completo:** permite a ambos extremos de una conexión transmitir en cualquier momento, incluso de manera simultánea.
- **Oportunidad:** El uso de temporizadores asegura que los datos se transmitan dentro de un tiempo razonable.
- **Orden:** Los datos enviados desde una aplicación se reciben en el mismo orden en el otro extremo. Esto ocurre a pesar del hecho de que los datagramas podrían recibirse en desorden a través del IP, debido a que el TCP reensambla el mensaje en el orden correcto antes de pasarlo a las capas superiores.
- **Etiquetado:** Todas las conexiones han acordado un valor de precedencia y seguridad.
- **Flujo controlado:** El TCP puede regular el flujo de información utilizando búfer y límites de ventana.
- **Corrección de errores:** La suma de verificación asegura que los datos están libres de errores (dentro de los límites del algoritmo de la suma de verificación).

PROTOCOLO ICMP

El ICMP es un sistema de reporte de errores. Es una parte integral del IP y debe incluirse en cada aplicación del IP. Éste proporciona mensajes y señales de error consistentes y comprensibles a lo largo de las versiones diferentes del IP y de sistemas operativos distintos. Es útil pensar en el ICMP como un paquete IP diseñado de manera específica para hablar con otro paquete IP a través de la red: en otras palabras, el ICMP es el sistema de comunicaciones de la capa IP. Los menajes generados por el ICMP los trata el resto de la red como cualquier otro datagrama IP, pero el software de la capa IP los interpreta en

forma diferente. Los mensajes ICMP tienen un encabezado incorporado de la misma manera que cualquier datagrama IP y, los datagramas ICMP no se diferencian en ningún punto de los datagramas transportadores de datos, hasta que la capa IP de la máquina receptora procesa el datagrama en forma apropiada.

En casi todos los casos, los mensajes de error enviados por el ICMP se enlutan de regreso a la máquina transmisora del datagrama original. Esto se debe a que sólo las direcciones IP del dispositivo de envío y de destino se incluyen en el encabezado. Debido a que el error no significa nada para el dispositivo de destino, el transmisor es el receptor lógico del mensaje de error. Entonces el transmisor puede determinar, a partir del mensaje ICMP, el tipo de error que ocurrió y establece la mejor forma de enviar de nuevo el datagrama que falló.

Los mensajes ICMP pasan por dos encapsulamiento, como todos los mensajes IP: incorporación en un datagrama IP regular y luego en el marco de red. Sin embargo, los encabezados ICMP tienen un formato diferente que los encabezados IP, y el formato difiere ligeramente, dependiendo del tipo de mensaje. No obstante, todos los encabezados ICMP comienzan con los mismos tres campos: un tipo de mensaje, un campo de código y una suma de verificación para el mensaje ICMP.

CUESTIONARIO PRELIMINAR

1. ¿Qué es el protocolo TCP y cómo funciona?
2. ¿Qué es u puerto y para qué sirve?
3. Describe la diferencia entre un puerto activo y un puerto pasivo.
4. ¿Qué es un temporizador TCP?
5. Describe brevemente los tipos de temporizadores TCP.
6. menciona las unidades de datos del protocolo TCP.
7. Describe brevemente que es OSI.
8. Menciona las similitudes del protocolo TCP y OSI.
9. ¿Qué es ICMP y cuál e su principal función?
10. Menciona el nombre de algún problema que pueda surgir en el enrutamiento de un mensaje del trasmisor al receptor.
11. ¿Para qué sirve el comando ping utilizado una terminal MS-DOS?
12. Menciona los parámetros del comando ping y para qué sirve cada uno de ellos.

HERRAMIENTAS Y RECURSOS

-1 equipo de cómputo por grupo de trabajo con Sistema Operativo Windows 98 y el software de Ethereal previamente instalado.
-Conexión a Internet
-Se pide a los alumnos los conocimientos suficientes para manejar S.O. Windows 98.
-Haber contestado el cuestionario preliminar.

*El material se encuentra en el laboratorio.

DESARROLLO

Ejercicio 1. Filtrado, Captura y Análisis del protocolo ICMP a través del comando ping.

Paso 1. Encienda el equipo que le haya sido asignado.

Paso 2. Cuando aparezca la ventana de *"Contraseña de Red"*, ingrese al ambiente Windows digitando en *"Nombre de Usuario"*el nombre de la PC y en el de *"Contraseña"* vuelva a escribir el nombre de la PC. Por ultimo de un clic en el botón de *"Aceptar"* o presione la tecla de *"Enter"*.

Paso 3. De doble clic sobre el icono del Ethereal para que se ejecute el programa.

Paso 4. Para poner un filtro de despliegue de un clic en el botón *"Expression..."* y a continuación se desplegara un cuadro de dialogo *"Ethereal: Filter expresión"* en la parte de *"Field name"* busque la opción ICMP y de un clic en la flecha que se encuentra a la izquierda del protocolo, del menú que sale elija la opción icmp.type_Type. A continuación en la parte de *"Relation"* de clic en el símbolo de = =, en la parte de *"Value"* escriba el número 8, de un clic en el botón de *"OK"* para guardar la opción del filtro.

Paso 5. Iniciar una captura dando un clic en el menú *"Capture"* y seleccionando *"Start"*.

Paso 6. *"Capture Filter"* a continuación se desplegara la ventana de *"Ethereal: Capture Filter"*. En la parte de *"Capture"* de un clic en la opciòn *"Capture Filter"*. A continuación en el área de *"Properties"* escriba en la parte de *"Filter name"* Captura1 y en la parte de *"Filter string"* src host (dirección IP de la máquina) y dar un clic en el botón *"Ok"*

Paso 7. En una ventana aparte, en una terminal de comandos MS-DOS, escribir
ping 132.248.173.148

Aguardar a que termine de ejecutarse el comando.

Paso 8. Terminar la captura presionando el botón de *"Stop"* en la ventana de captura de Ethereal.

Paso 9. Examinar la captura. Reconocer los paquetes pedidos.

Paso 10. De la ventana de *"Resumen de paquetes capturados"* elegir un paquete y dar clic sobre él.

Paso 11. A continuación escriba los datos obtenidos en esta ventana de uno de los paquetes.

No.
Time
Source
Destination
Protocol
Info

Paso 12. Describa con sus propias palabras cada uno de los datos obtenidos.

Paso 13. De una conclusión breve de los datos analizados.

Paso 14. Escriba los datos obtenidos de la ventana *"Detalles de encabezado de protocolos para el paquete seleccionado"*. De un clic en el signo de "+" de la parte que corresponde al protocolo ICMP. Anote todos los detalles.

Paso 15. Describa con sus propias palabras cada uno de los detalles obtenidos.

Paso 16. De una conclusión breve de los datos.

Como te darás cuenta Ping es una herramienta de diagnóstico para verificar la conectividad entre dos computadoras en una red. Envía paquetes ICMP con Respuesta de Eco a una dirección IP remota y observa las respuestas ICMP, en el ejemplo anterior se ve claramente como las dos computadoras tienen conectividad.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	132.248.173.174	Broadcast	ARP	Who has 132.248.173.
2	0.000250	132.248.173.148	132.248.173.174	ARP	132.248.173.148 is
3	0.000261	132.248.173.174	132.248.173.148	ICMP	Echo (ping) request
4	0.000577	132.248.173.148	132.248.173.174	ICMP	Echo (ping) reply
5	0.996863	132.248.173.174	132.248.173.148	ICMP	Echo (ping) request
6	0.997158	132.248.173.148	132.248.173.174	ICMP	Echo (ping) reply
7	1.998281	132.248.173.174	132.248.173.148	ICMP	Echo (ping) request

Paso 17. Repita los pasos 3 al 16 utilizando la misma información, en este caso se utilizará una dirección de host de destino inalcanzable.

Paso 18. A continuación de la ventana *"Resumen de paquetes capturados"* escriba los datos obtenidos de uno de los paquetes del protocolo ICMP que corresponda en la parte de la Información a Destination Unreachable.

No.
Time
Source
Destination
Protocol
Info

Paso 12. Describa con sus propias palabras cada uno de los datos obtenidos.

Paso 13. De una conclusión breve de los datos analizados.

Paso 14. Escriba los datos obtenidos del mismo paquete de la ventana *"Detalles de encabezado de protocolos para el paquete seleccionado"*. De un clic en el signo de "+" de la parte que corresponde al protocolo ICMP. Anote todos los detalles.

Paso 15. Describa con sus propias palabras cada uno de los detalles obtenidos.

Paso 16. De una conclusión breve de los datos.

Como se dio cuenta no fue el mismo resultado obtenido anteriormente ya que no se obtuvo conectividad entre estas dos computadoras por lo que ICMP manda un mensaje de Destino inalcanzable (verifique Tabla 2 del marco teórico).

Ejercicio 2. Filtrado, Captura y Análisis del protocolo TCP a través del servicio Telnet.

Paso 4. Para poner un filtro de despliegue de un clic en el botón *"Expression..."* y a continuación se desplegara un cuadro de dialogo *"Ethereal: Filter expresión"* en la parte de *"Field name"* busque la opción TCP y de un clic en ella, de un clic en el botón de *"OK"* para guardar la opción del filtro.

Paso 5. Iniciar una captura dando un clic en el menú *"Capture"* y seleccionando *"Start"*.

Paso 6. *"Capture Filter"* a continuación se desplegara la ventana de *"Ethereal: Capture Filter"*. En la parte de *"Capture"* de un clic en la opción *"Capture Filter"*. A continuación en el área de *"Properties"* escriba en la parte de *"Filter name"* Captura2 y en la parte de *"Filter string"* host (dirección IP de la máquina) y dar un clic en el botón *"Ok"*

Paso 5. En una ventana aparte, en una terminal de comandos MS-DOS, ejecutar un telnet con los datos que su instructor le indique.

Aguardar a que termine de ejecutarse el comando.

Paso 6. Terminar la captura presionando el botón de *"Stop"* en la ventana de captura de Ethereal.

Paso 7. Examinar la captura. Reconocer los paquetes pedidos.

Paso 8. De la ventana de *"Resumen de paquetes capturados"* elegir un paquete y dar clic sobre él.

Paso 9. Analice cada uno de los paquetes obtenidos y específicamente analice la parte que corresponde al protocolo TCP, con sus propias palabras y de acuerdo a los datos obtenidos explique el establecimiento de la conexión (observe la parte del marco teórico que corresponde a Unidades de datos del protocolo TCP).

Al analizar cada uno de los paquetes que corresponden a TELNET se dará cuenta como funciona esta aplicación del protocolo TCP/IP, ya que va mostrando paso a paso la forma en como establece la conexión. La forma más sencilla de hacerlo es en la parte de la ventana *"Detalles de encabezado de protocolos para el paquete seleccionado"*. Dé un clic en la flecha de la parte que corresponde al servicio Telnet.

Una de las funciones básicas cuando se usa Internet es conectarse y trabajar en otra computadora de la red. Esto es posible a través del comando *telnet*. Telnet es una aplicación del protocolo (TCP/IP) que permite la conexión y uso de un servidor remoto. Permite acceder a servicios tales como:

- Bases de datos
- Catálogos de Acceso Público en Línea
- Directorios de direcciones de correo electrónico
- Clima

Existen dos niveles básicos de servicio de Telnet:

1. Cuenta tipo Invitado (Guest). También conocida como Acceso Público. Permite hacer una conexión a un servidor remoto y usar cualquier "servicio público" que esté disponible.
2. Cuenta con Privilegios completos. Este nivel permite hacer una conexión a cualquier servidor en el que el usuario tenga cuenta y contraseña.

Ejemplo:

login:alma
password:hawk

Como Telnet es un servicio del conjunto de protocolos TCP/IP, en el mercado existen implementaciones de este protocolo en diferentes plataformas como: Unix, Microsoft Windows,VMS, etc., la sintaxis del comando cambia, así como algunas instrucciones dependiendo del sistema operativo.

Ejercicio 2. Filtrado, Captura y Análisis del protocolo TCP a través del servicio Secure Shell (SSH).

Paso 1. Para poner un filtro de despliegue de un clic en el botón *"Expression..."* y a continuación se desplegara un cuadro de dialogo *"Ethereal: Filter expresión"* en la parte de *"Field name"* busque la opción TCP y de un clic en ella, de un clic en el botón de *"OK"* para guardar la opción del filtro.

Paso 2. Iniciar una captura dando un clic en el menú *"Capture"* y seleccionando *"Start"*.

Paso 3. *"Capture Filter"* a continuación se desplegara la ventana de *"Ethereal: Capture Filter"*. En la parte de *"Capture"* de un clic en la opción *"Capture Filter"*. A continuación en el área de *"Properties"* escriba en la parte de *"Filter name"* Captura3 y en la parte de *"Filter string"* host (dirección IP de la máquina) y dar un clic en el botón *"Ok"* y otro clic en la pantalla *"Ethereal: Capture options"*, para que se inicie la captura.

Paso 4. En una ventana aparte, en una terminal de SSH Secure File Transfer Client, ejecutar una conexión a un host remoto con los datos que su instructor le indique.

Aguardar a que termine de ejecutarse el comando.

Paso 5. Terminar la captura presionando el botón de *"Stop"* en la ventana de captura de Ethereal.

Paso 6. Examinar la captura. Reconocer los paquetes pedidos.

Paso 7. De la ventana de *"Resumen de paquetes capturados"* elegir un paquete y dar clic sobre él.

Paso 8. Analice cada uno de los paquetes obtenidos y específicamente analice la parte que corresponde al protocolo TCP. Con sus propias palabras y de acuerdo a los datos obtenidos explique el establecimiento de la conexión con SSH (observe la parte del marco teórico que corresponde a Unidades de datos del protocolo TCP).

Al analizar cada uno de los paquetes que corresponden a SSH se dará cuenta como funciona esta aplicación del protocolo TCP/IP.

SSH es un programa para conectarse a otros equipos a través de una red, para ejecutar comandos en una máquina remota y para mover archivos de una máquina a otra.
SSH provee comunicación segura sobre un canal inseguro y se puede ver como un reemplazo a los comandos **telnet, ftp, rlogin, rsh, y rcp**, los cuales proporcionan gran flexibilidad en la administración de una red pero presenta grandes riesgos en la seguridad de un sistema, lo cual no sucede en SSH ya que realiza la comunicación y transferencia de información de forma cifrada proporcionando fuerte autenticación sobre el medio inseguro.

Hagamos una pequeña comparación de cómo funciona Telnet y SSH:

Recordemos primeramente que FTP tiene como propósito principal transferir archivos desde una computadora hacia otra copiando y moviendo archivos desde los servidores hacia los clientes, y desde los clientes hacia los servidores, para lo cual necesita un servicio de conexión entre computadoras.
Telnet realiza la conexión, transmitiendo las pulsaciones del teclado una por una al host remoto y enviando el resultado de pantalla nuevamente al host local, imprimiéndolo en la pantalla. Compruebe verificando los paquetes obtenidos en el ejercicio 2 (Telnet) en los cuales se ve claramente que cada letra del password es visible a la red. En cambio con SSH el password viaja a través de la red en forma encriptada y no es posible obtenerlo en los datos capturados (en los paquetes obtenidos en la realización del ejercicio identifíquense como encrypted request packet y encrypted response packet).

Ejercicio 3. Filtrado, Captura y Análisis del protocolo TCP a través del FTP.

Paso 4. Para poner un filtro de despliegue de un clic en el botón *"Expression..."* y a continuación se desplegara un cuadro de dialogo *"Ethereal: Filter expresión"* en la parte de *"Field name"* busque la opción TCP y de un clic en ella, de un clic en el botón de *"OK"* para guardar la opción del filtro.

Paso 5. Iniciar una captura dando un clic en el menú *"Capture"* y seleccionando *"Start"*.

Paso 6. *"Capture Filter"* a continuación se desplegara la ventana de *"Ethereal: Capture Filter"*. En la parte de *"Capture"* de un clic en la opción *"Capture Filter"*. A continuación en el área de *"Properties"* escriba en la parte de *"Filter name"* Captura2 y

en la parte de *"Filter string"* host (dirección IP de la máquina) y dar un clic en el botón *"Ok"*

Paso 5. En una ventana aparte, en una terminal de comandos MS-DOS, ejecute el comando de FTP y conéctese a una terminal con los datos que su instructor le indique.

Aguardar a que termine de ejecutarse el comando.

Paso 6. Terminar la captura presionando el botón de *"Stop"* en la ventana de captura de Ethereal.

Paso 7. Examinar la captura. Reconocer los paquetes pedidos.

Paso 8. De la ventana de *"Resumen de paquetes capturados"* elegir un paquete y dar clic sobre él.

Paso 9. Analice cada uno de los paquetes obtenidos y específicamente analice la parte que corresponde al protocolo TCP, con sus propias palabras y de acuerdo a los datos obtenidos explique el establecimiento de la conexión (observe la parte del marco teórico que corresponde a Unidades de datos del protocolo TCP).

CUESTIONARIO

1. Defina la multiplexión y cómo se usaría para combinar tres máquinas fuente con una máquina destino. Relaciónelo con los números de puerto.

2. ¿Qué son los números de puerto y sockets?

3. Describa los temporizadores usados con el TCP.

4. ¿Cuáles son los seis subservicios de transporte de datos ofrecidos por el TCP?

5. Use un diagrama para mostrar las señales que intervienen en dos máquinas que establecen una conexión TCP. Luego, muestre cómo se transfieren los datos. Por último, muestre el proceso de terminación.

6. Dé una descripción del ICMP en una oración.

7. ¿Cómo se crea un datagrama de mensaje de ICMP?

8. Los encabezados ICMP son bastante pequeños. Muestre la estructura de un encabezado de mensaje común y el significado de los bits que contiene.

CONCLUSIONES

Que el alumno haga un análisis de cada uno de los pasos que llevo a cabo y comente dudas y haga aclaraciones de todo lo que pudo aprender en esta práctica.

CONCLUSIONES

Como sabemos las computadoras han sido una de las principales tecnologías de la que más ha sido notoria su evolución e impacto en la sociedad. En estos tiempos es casi obligatoria la utilización de las redes de computadoras dentro de las pequeñas y grandes empresas y organizaciones. Para realizar procesos en donde se intercambie información, se compartan recursos y se optimicen tiempos. No obstante, existen empresas donde su forma de trabajar aún continua siendo obsoleta debido a que la actualización y la modernidad no se ha hecho presente, pero también es cierto que cada vez más la mentalidad de trabajar eficaz y eficientemente junto con la necesidad de resistir ante la competencia despierta una inquietud de actualización en cada organización empresa que cada vez más se convierte en necesidad.

Las universidades siguen aumentando considerablemente sus matrículas en carreras de tecnologías de comunicaciones y computación debido a la considerable demanda de los alumnos. El punto relevante y a tratar es analizarse si los alumnos que egresan poseen los conocimientos necesarios para cubrir las necesidades que exige el sector laboral en un profesionista de tales caracteristieas.

Se concluye que para el caso de la carrera de Ingeniería en Computación impartida en la Escuela Nacional de Estudios Profesionales plantel Aragón (UNAM), el nivel de conocimientos de redes de computadoras adquirido por los alumnos es deficiente en el aspecto de que los alumnos puedan desarrollar la parte práctica dentro del ámbito laboral. Para poder mejorar el conocimiento adquirido en la parte teórica se deberá renovar los programas de ésta asignatura en la carrera. Se considera importante también la implantación de un laboratorio de redes que refuerce lo visto en teoría, con prácticas que ayuden al alumno a familiarizarse con lo que seguramente se enfrentará en el mercado laboral.

Los recursos materiales que dispone la carrera citados en la tesis forman parte de la base para la creación del laboratorio. Es importante señalar que una buena parte de la población estudiantil esta de acuerdo en cooperar y auxiliar en el establecimiento de este laboratorio aportando parte de su tiempo, esfuerzo y ayuda monetaria.

Referente a las prácticas y a los objetivos de cada una, fueron desarrolladas en base al tema de protocolos TCP/IP que es solo una parte del temario de la materia de Redes de Computadoras, se diseñaron de tal manera que se puedan desarrollar durante las clases del tema que corresponde a Protocolos.

Cada uno de los temas que corresponden a las prácticas está relacionado directamente con el temario de la materia de redes y complementado con el perfil propuesto por el ANIEI. Otro aspecto importante que fue tomado en cuenta para elaborar cada una de las

prácticas, es la utilidad de cada herramienta, procedimiento y aplicaciones que en a los alumnos se les podrá presentar en dentro de su ámbito laborar.

Es importante señalar que las redes de computadoras no puede ser visto de manera detallada en todos sus temas en solo semestre, existen temas que por lo extenso que resultan y debido a la complejidad que presentan así como los altos costos que implica utilizar estas tecnologías no se contemplan dentro del análisis en el laboratorio de redes.

De la misma forma en que se propone la actualización de la materia, de esa manera se propone la actualización del equipo y de las prácticas en el laboratorio constantemente para poder abarcar una mayor área de conocimientos, además de esa manera se pueden ir cubriendo cada uno de los temas que actualmente no estén complementados.

Otro aspecto importante en donde el laboratorio de redes tendría un peso específico sería en las habilidades que el alumno pueda desarrollar en él mismo, habilidades que estarán fundamentadas con la teoría y recomendaciones del profesor. El primer objetivo de estas prácticas es involucrar al alumno con las necesidades que exigen el manejo de las redes actuales.

Tomando en cuenta que las redes de computadoras evolucionan día a día tanto en software como en hardware es de suma importancia que las prácticas se vayan actualizando conforma pase el tiempo y surjan nuevos y avanzados programas de tal forma que el alumno siempre este a la vanguardia en información y conocimientos adquiridos en esta materia. La idea es crear una base de prácticas con los recursos que se tienen actualmente y mejorarlos de acuerdo a las posibilidades de la institución.

El laboratorio puede apoyar no solo a la materia de redes, y aunque ese es nuestro propósito principal, también puede ser tomado en cuenta en cursos de apoyo para otras asignaturas relacionadas con el área que necesiten reforzarse.

Tanto las prácticas como el laboratorio deberán ser capaces de adaptarse a los cambios que las tecnologías reflejen y ayudará al alumno a tener una mejor visión de los conceptos que la parte teórica le ofrezca, además de poder absorber de mejor manera los cambios que existan en el mundo de las computadoras.

ANEXO A

Puertos, RFC's y Siglas

Cada proceso que se desea comunicar con otro se identifica en la pila de protocolos TCP/IP con uno o más puertos. Un puerto es un número de 16 bits, empleado por un protocolo host – a – host para identificar a que protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos.

Como algunas aplicaciones son ya de por sí protocolos estandarizados, como TELNET y FTP, emplean el mismo número de puerto en todas las implementaciones TCP/IP. Estos puertos "asignados" se conocen como puertos bien conocidos, y a sus aplicaciones, aplicaciones bien conocidas.

Estos puertos son controlados y asignados por IANA ("Internet Assigned Numbers Authority") y en la mayoría de los sistemas sólo los puede utilizar los procesos del sistema o los programas que ejecutan usuarios privilegiados. Ocupan número de puerto comprendidos en el rango de 0 a 1023. Los puertos con números en el rango de 1024 a 65535 no los controla IANA y en la mayor parte de los sistemas los pueden usar los programas de usuario.

La confusión que se produce cuando dos aplicaciones distintas intentan usar los mismos puertos en un host se evita haciendo que soliciten un puerto disponible a TCP/IP. Como este número se asigna dinámicamente, puede ser diferente en cada ejecución de una misma aplicación.

Los números de puerto tienen los siguientes intervalos asignados:

- Los números inferiores a 255 se usan para aplicaciones públicas.
- Los números del 255 al 1023 son asignados a empresas para aplicaciones comercializables.
- Los números superiores a 1023 no están regulados, y se usan generalmente para asignación dinámica.

Cuando una aplicación cliente quiere comunicarse con una aplicación servidora de otro host busca un número de puerto libre y lo utiliza para transmitir los datos, mientras que en el otro host la aplicación servidora permanece a la escucha en su puerto bien conocido para recibir los datos. Por ejemplo, cualquier conversación destinada a la aplicación FTP utiliza el número de puerto estándar 21.

Los puertos bien conocidos y sus aplicaciones asociadas se definen en RFC1700, y se presentan en la siguiente tabla:

número	clave WINDOWS	clave UNIX	descripción
0/TCP			reservado
0/UDP			reservado
1/TCP	TCPMUX		Multiplexor TCP
5/TCP	RJE		Introducción de función remota de tareas
7/TCP-UDP	ECHO	echo	Eco
9/TCP-UDP	DISCARD	discard	Abandonar
11/TCP-UDP	ACTIVE USERS	systat	Usuarios activos
13/TCP-UDP	DAYTIME	daytime	Fecha, hora
15		netstat	Estado de la red. ?Quién está conectado?
17/TCP-UDP	QOTD	qotd	Cita del día
19/TCP-UDP	CHARGEN	chargen	Generador de caracteres
20/TCP	FTP-DATA	ftp-data	Protocolo de transferencia de ficheros (datos)
21/TCP	FTP	ftp	Protocolo de transferencia de ficheros
23/TCP	TELNET	telnet	Conexión por terminal
25/TCP	SMTP	smtp	Protocolo de transporte de correo sencillo
37/TCP-UDP	TIME	time	Hora-fecha
39/TCP-UDP	RLP		Protocolo de ubicación de recursos
42/TCP-UDP	NAMESERVER	name	Servidor de nombres de host
43/TCP-UDP	NICNAME	whois	Comando whois. ?Quién es?
53/TCP-UDP	DOMAIN	nameserver	Servidor de nombres de dominio (DNS)
67/TCP-UDP	BOOTPS	bootps	Servidor de protocolo Bootstrap
68/TCP-UDP	BOOTPC	bootpc	Cliente de protocolo Bootstrap
69/UDP	TFTP	tftp	Transferencia de ficheros trivial
70/TCP	GOPHER	gopher	Gopher
75/TCP			Cualquier servicio privado de conexión telefónica
77/TCP			Cualquier servicio RJE privado
79/TCP	FINGER	finger	Comando figer
80/TCP	WWW-HTTP	www-http	World Wide Web HTTP (servicio de páginas web)
93/TCP	DCP		Protocolo de Control de Dispositivo
95/TCP	SUPDUP	supdup	Protocolo SUPDUP
101/TCP	HOSTNAME	hostnames	Servidor de nombre de host NIC
102	ISO-TSAP		ISO-TSAP
103/TCP	X400	x400	Servicio de correo X400
104/TCP	X400-SND	x400-snd	Envío de correo X400
107/TCP-UDP	RTELNET	rtelnet	Telnet remoto
109/TCP	POP2	pop2	Post Office Protocol - Versión 2
110/TCP	POP3	pop3	Post Office Protocol - Versión 3
111/TCP-UDP	SUNRPC	sunrpc	Sun Remote Procedure Call
113/TCP	AUTH	auth	Servicio de autenticación
115/TCP-UDP	SFTP	sftp	Protocolo de Transferencia de Ficheros Simple
117/TCP-UDP	UUCP-PATH		Servicio de ruta UUCP
119/TCP	NNTP	nntp	Protocolo de Transferencia de Noticias en Red
123/UDP	NTP	ntp	Network Time Protocol (Protocolo de tiempo de red)
129/TCP	PWDGEN	pwdgen	Protocolo Generador de Contraseñas
137/TCP-UDP	NETBIOS-NS		Servicio de Nombres NETBIOS
138/TCP-UDP	NETBIOS-DGM		Servicio de Datagramas NETBIOS

139/TCP-UDP	NETBIOS-SSN		Servicio de Sesión NETBIOS
161/UDP	SNMP		SNMP
162/UDP	SNMPTRAP		SNMPTRAP
194/TCP	IRC	irc	Internet Relay Chat Protolol (Protocolo de Internet para Chat)

RFC declarados como estándares.

La mayor parte de la información acerca de la familia de protocolos TCP/IP está publicada como Peticiones de comentarios (Request For Commnets, RFCs). Las RFC definen los distintos aspectos del protocolo, su utilización y la administración como un conjunto de notas vagamente ordenadas.

Las RFC contienen una gran cantidad de información sin aplicación, pero también contienen un cúmulo de detalles para los que desean llevar a TCP/IP a sus límites.

Cómo acceder a las RFC

Las RFC pueden obtenerse de diferentes formas, la más fácil de estas es la electrónica. Las copias en papel están disponibles bajo pedido. Las copias electrónicas están generalmente en formato ASCII, aunque algunas están en formato PostScrip y requieren un intérprete para imprimirlas. La mayor parte de las RFC obtenidas electrónicamente no tienen diagramas, figuras ni fotos.

Cómo acceder a las RFC a través del FTP

Las RFC pueden obtenerse utilizando FTP a través del Internet Network Information Center (NIC). Utilice FTP para obtener el acceso al acervo NIC llamado NIC.DDN.MIL. utilice el nombre de usuario guest y la contraseña anonymous. Las RFC pueden resupaerarse utilizando el comando FTP get con el siguiente formato:

<RFC>RFC527.txt

Reemplace la parte RFC527 con el número de la RFC requerida. Se puede utilizar FTP dentro del archivo NIC, sólo si tiene acceso a una máquina con acceso a Internet.

Cómo acceder a las RFC a través del correo electrónico.

Las RFC pueden solicitarse a través de correo electrónico. Tanto NIC como el NSFNET Network Service Center proporcionan respuestas automatizadas, regresando la RFC solicitada. Ambos servicios leen el correo electrónico entrante para localizar las palabras clave que indiquen qué RFC se solicita, así como la dirección de correo electrónico del remitente y, luego, envían la RFC requerida.

Para obtener una RFC de NIC, envíe un mensaje con el campo de teme indicando la RFC que desea. Envíelo a service@nic.ddn.mil. Si quiere más datos sobre cómo obtener la información a través del sistema de correo electrónico de NIC, envíe un correo con la palabra help como tema.

Para obtener RFC desde el NSFNET Network Service Center, envíe un mensaje con las primeras dos líneas, como éstas:

REQUEST: RFC
TOPIC: 527

La primera línea especifica que usted quiere una RFC y la segunda línea da el número de RFC. Envíe el correo electrónico a info-server@sh.cs.net. Para mayor información, escriba help en el campo del tema.

Cómo acceder a las copias impresas de las RFC

Si usted no tiene acceso a las comunicaciones electrónicas, puede solicitar una copia previamente impresa de una RFC. Para obtener una copia impresa de cualquier RFC, llame al Network Information Center al 1-800-235-3155.

Se considera de mala educación hacer esperar al equipo del NIC, mientras usted encuentra qué RFC quiere. Primero haga una lista de ellas, de manera que su conversación telefónica sea corta y concisa. Ellos deben contestar muchas llamadas al día y por lo general están bastante ocupados.

RFC0768-ES	**Protocolo UDP**	ESTÁNDAR	STD0006
RFC0774-ES	**Guía del Protocolo de Internet**	---	---
RFC0791-ES	**Protocolo IP**	ESTÁNDAR	STD0005
RFC0792-ES	**Protocolo ICMP**	ESTÁNDAR	STD0005
RFC0793-ES	**Protocolo TCP**	ESTÁNDAR	STD0007
RFC0805-ES	**Apuntes del Congreso de Correo**	DESCONOCIDO	---

	por Ordenador		
RFC0854-ES	**Especificación del protocolo Telnet**	ESTÁNDAR	STD0008
RFC0855-ES	**Especificaciones de opción Telnet**	ESTÁNDAR	STD0008
RFC0856-ES	**Transmisión binaria en Telnet**	ESTÁNDAR	STD0027
RFC0857-ES	**Opción Eco de Telnet**	ESTÁNDAR	STD0028
RFC0862-ES	**Protocolo de Eco**	ESTÁNDAR	STD0020
RFC0863-ES	**Protocolo de Descarte**	ESTÁNDAR	STD0021
RFC0864-ES	**Protocolo Generador de Caracteres**	ESTÁNDAR	STD0022
RFC0865-ES	**Protocolo de Cita del Día**	ESTÁNDAR	STD0023
RFC0866-ES	**Usuarios Activos**	ESTÁNDAR	STD0024
RFC0867-ES	**Protocolo de Hora Diaria**	ESTÁNDAR	STD0025
RFC0868-ES	**Protocolo de Hora**	ESTÁNDAR	STD0026
RFC0919-ES	**Difusión de Datagramas de Internet**	ESTÁNDAR	STD0005
RFC0922-ES	**Difusión de datagramas en internet en presencia de subredes**	ESTÁNDAR	STD0005
RFC0950-ES	**Procedimiento Estándar para División en Subredes en Internet**	ESTÁNDAR	STD0005
RFC0953-ES	**Servidor de Nombres de Máquinas**	HISTÓRICO	---
RFC0959-ES	**Protocolo FTP**	ESTÁNDAR	STD0009
RFC0974-ES	**Encaminamiento de correo y el sistema de dominios**	ESTÁNDAR	STD0014
RFC1178-ES	**Cómo elegir un nombre para su ordenador**	INFORMATIVO	FYI0005
RFC1219-ES	**Sobre la asignación de números de subred**	INFORMATIVO	---
RFC1234-ES	**Encaminamiento del Tráfico IPX a través de redes IP**	ESTÁNDAR PROPUESTO	---
RFC1459-ES	**Protocolo IRC**	EXPERIMENTAL	---
RFC1591-ES	**Estructura y delegación del sistema de nombres de dominio (DNS)**	INFORMATIVO	---
RFC1597-ES	**Asignación de Direcciones para Internets privadas (obsoleto)**	INFORMATIVO	Actualizado por RFC1918
RFC1738-ES	**Localizadores Uniformes de Recursos (URL)**	SEGUIMIENTO de ESTÁNDAR	Actualizado por RFC1808, RFC2368, RFC2396
RFC1780-ES	**Estándares Oficiales de Protocolos de Internet**	SEGUIMIENTO de ESTÁNDAR	STD0001
RFC1886-ES	**Extensiones DNS para dar soporte a IPv6**	ESTÁNDAR PROPUESTO	---
RFC1918-ES	**Asignación de direcciones para Internet privadas**	MEJOR PRÁCTICA ACTUAL	BCP0005
RFC1928-ES	**Protocolo SOCKS Versión 5**	ESTÁNDAR PROPUESTO	---

RFC1929-ES	**Autentificación mediante Usuario/Palabra clave para el protocolo SOCKS V5**	ESTÁNDAR PROPUESTO	---
RFC1939-ES	**Protocolo POP3**	ESTÁNDAR	STD0053
RFC2045-ES	**Extensiones Multipropósito al Correo de Internet (MIME) Primera Parte:**	BORRADOR DE ESTÁNDAR	---
RFC2046-ES	**Extensiones Multipropósito al Correo de Internet (MIME) Segunda Parte:**	BORRADOR DE ESTÁNDAR	---
RFC2047-ES	**MIME, Tercera Parte: Extensiones de la cabecera de los mensajes para texto no-ASCII**	BORRADOR DE ESTÁNDAR	---
RFC2060-ES	**Protocolo IMAP – Versión 4rev1**	ESTÁNDAR PROPUESTO	---
RFC2119-ES	**Palabras clave a utilizar en RFC para Indicar Niveles de Requerimiento**	MEJOR PRÁCTICA ACTUAL	BCP0014
RFC2223-ES	**Instrucciones para autores de RFC**	INFORMATIVO	---
RFC2460-ES	**Especificación del Protocolo Internet, Versión 6 (Ipv6)**	BORRADOR DE ESTÁNDAR	---
RFC2462-ES	**Configuración Automática sin Estado de Direcciones Ipv6**	BORRADOR DE ESTÁNDAR	---
RFC2606-ES	**Nombres DNS reservados de primer nivel**	MEJOR PRÁCTICA ACTUAL	BCP0032
RFC2663-ES	**Terminología y consideraciones sobre Traducción de Direcciones IP**	INFORMATIVO	---
RFC2694-ES	**Extensiones del DNS para Traductores de Direcciones de Red (DNS_ALG)**	INFORMATIVO	---
RFC	**DESCRIPCIÓN**	ESTADO	TAMBIÉN
RFC0768-ES	**Protocolo UDP**	ESTÁNDAR	STD0006
RFC0774-ES	**Guía del Protocolo de Internet**	---	---
RFC0791-ES	**Protocolo IP**	ESTÁNDAR	STD0005
RFC0792-ES	**Protocolo ICMP**	ESTÁNDAR	STD0005
RFC0793-ES	**Protocolo TCP**	ESTÁNDAR	STD0007
RFC0805-ES	**Apuntes del Congreso de Correo por Ordenador**	DESCONOCIDO	---
RFC0854-ES	**Especificación del protocolo Telnet**	ESTÁNDAR	STD0008
RFC0855-ES	**Especificaciones de opción Telnet**	ESTÁNDAR	STD0008
RFC0856-ES	**Transmisión binaria en Telnet**	ESTÁNDAR	STD0027
RFC0857-ES	**Opción Eco de Telnet**	ESTÁNDAR	STD0028
RFC0862-ES	**Protocolo de Eco**	ESTÁNDAR	STD0020
RFC0863-ES	**Protocolo de Descarte**	ESTÁNDAR	STD0021

RFC0864-ES	**Protocolo Generador de Caracteres**	ESTÁNDAR	STD0022
RFC0865-ES	**Protocolo de Cita del Día**	ESTÁNDAR	STD0023
RFC0866-ES	**Usuarios Activos**	ESTÁNDAR	STD0024
RFC0867-ES	**Protocolo de Hora Diaria**	ESTÁNDAR	STD0025
RFC0868-ES	**Protocolo de Hora**	ESTÁNDAR	STD0026
RFC0919-ES	**Difusión de Datagramas de Internet**	ESTÁNDAR	STD0005
RFC0922-ES	**Difusión de datagramas en internet en presencia de subredes**	ESTÁNDAR	STD0005
RFC0950-ES	**Procedimiento Estándar para División en Subredes en Internet**	ESTÁNDAR	STD0005
RFC0953-ES	**Servidor de Nombres de Máquinas**	HISTÓRICO	---
RFC0959-ES	**Protocolo FTP**	ESTÁNDAR	STD0009
RFC0974-ES	**Encaminamiento de correo y el sistema de dominios**	ESTÁNDAR	STD0014
RFC1178-ES	**Cómo elegir un nombre para su ordenador**	INFORMATIVO	FYI0005
RFC1219-ES	**Sobre la asignación de números de subred**	INFORMATIVO	---
RFC1234-ES	**Encaminamiento del Tráfico IPX a través de redes IP**	ESTÁNDAR PROPUESTO	---
RFC1459-ES	**Protocolo IRC**	EXPERIMENTAL	---
RFC1591-ES	**Estructura y delegación del sistema de nombres de dominio (DNS)**	INFORMATIVO	---
RFC1597-ES	**Asignación de Direcciones para Internets privadas (obsoleto)**	INFORMATIVO	Actualizado por RFC1918
RFC1738-ES	**Localizadores Uniformes de Recursos (URL)**	SEGUIMIENTO de ESTÁNDAR	Actualizado por RFC1808, RFC2368, RFC2396
RFC1780-ES	**Estándares Oficiales de Protocolos de Internet**	SEGUIMIENTO de ESTÁNDAR	STD0001
RFC1886-ES	**Extensiones DNS para dar soporte a Ipv6**	ESTÁNDAR PROPUESTO	---
RFC1918-ES	**Asignación de direcciones para Internet privadas**	MEJOR PRÁCTICA ACTUAL	BCP0005
RFC1928-ES	**Protocolo SOCKS Versión 5**	ESTÁNDAR PROPUESTO	---
RFC1929-ES	**Autentificación mediante Usuario/Palabra clave para el protocolo SOCKS V5**	ESTÁNDAR PROPUESTO	---
RFC1939-ES	**Protocolo POP3**	ESTÁNDAR	STD0053
RFC2045-ES	**Extensiones Multipropósito al Correo de Internet (MIME) Primera Parte:**	BORRADOR DE ESTÁNDAR	---

RFC2046-ES	**Extensiones Multipropósito al Correo de Internet (MIME) Segunda Parte:**	BORRADOR DE ESTÁNDAR	---
RFC2047-ES	**MIME, Tercera Parte: Extensiones de la cabecera de los mensajes para texto no-ASCII**	BORRADOR DE ESTÁNDAR	---
RFC2060-ES	**Protocolo IMAP – Versión 4rev1**	ESTÁNDAR PROPUESTO	---
RFC2119-ES	**Palabras clave a utilizar en RFC para Indicar Niveles de Requerimiento**	MEJOR PRÁCTICA ACTUAL	BCP0014
RFC2223-ES	**Instrucciones para autores de RFC**	INFORMATIVO	---
RFC2460-ES	**Especificación del Protocolo Internet, Versión 6 (Ipv6)**	BORRADOR DE ESTÁNDAR	---
RFC2462-ES	**Configuración Automática sin Estado de Direcciones Ipv6**	BORRADOR DE ESTÁNDAR	---
RFC2606-ES	**Nombres DNS reservados de primer nivel**	MEJOR PRÁCTICA ACTUAL	BCP0032
RFC2663-ES	**Terminología y consideraciones sobre Traducción de Direcciones IP**	INFORMATIVO	---
RFC2694-ES	**Extensiones del DNS para Traductores de Direcciones de Red (DNS_ALG)**	INFORMATIVO	---

Siglas

Siglas	Explicación
ACB	Acces Control Block (Bloque de Control de Acceso)
ACK	Acknowledgment (Acuse de recibo)
AF	Address Family (Familia e Dirección)
ANSI	American Nacional Standard Institute (Instituto Nacional Americano de Estándares)
API	Application Programming Interface (Interfaz para Programación de Aplicación)
ARP	Address Resolution Protocol (Protocolo para Definición de Dirección)
ARPA	Advanced Research Projects Agency (Agencia de Proyectos de

	Investigación Avanzada)
AS	Autonomous System (Sistema Autónomo)
ASA	American Standard Association (Asociación Americana de Estándares)
ASCII	American Nacional Standard Code for Information Interchange (Código Estándar Americano para Intercambio de Información)
ASN.1	Abstract Syntax Notation One (Notación Uno para Sintaxis Abstracta)
BBN	Bolt,Beranek,and Newman, Incorporated
BER	Basic Encoding Rules (Reglas Básicas para la Codificación)
BGP	Border Gateway Protocol (Protocolo para Gateway Fronterizo)
BSD	Berkeley Software Distribution
CMIPr	Common Management Information Protocol (Protocolo Común para Administración de Información)
CMIS	Common Management Information Service (Servicios Comunes para Administración de Información)
SMOT	Common Management Information Service and Protocol over TCP/IP (Servicios y Protocolo Comunes para Administración de Información sobre TCP/IP)
CRC	Cyclic Redundancy Check (Verificación de Redundancia Cíclica)
CSMA/CD	Carrier Sense Multiple Acces with Collision Detection (Acceso Múltiple de Detección de Portación con Detección de Colisión)
DARPA	Defense Advanced Research Project (Proyecto para Investigación Avanzada de Defensa)
DCA	Defense Communications Agency (Agencia de Comunicaciones de la Defensa)
DCE	Distributed Computing Enviroment (Ambiente de Computación Distribuida)
DCE	Data Circuit-Terminating Equipment (Equipo para Circuito de Terminación de Datos). También llamado Data Comunication Equipment (Equipo para Comunicaciones de Datos).
DES	Defense Encryption Standad (Estándar para Encriptación de Datos).
DFS	Distribuited File SErvice (Servicio de Archivos Distribuidos)
DISA	Defense Information Systems Agency (Agencia para Sistemas de Información de la Defensa).
DIX	Digital, Intel and Xerox Ethernet Protocol (Protocolo Ethernet de Didigital, Intel y Xerox).
DME	Distributed Management Enviroment (Ambiente de Administración Distribuida).
DNS	Domain Name Service (Servicio de Nombre de Dominio).
DSAP	Destination Service Access Point (Punto Destino para Acceso al Servicio).
DTE	Data Terminal Equipment (Equipo para Terminal de Datos).
DUA	Directory User Agent (agente para Usuario de Directorio).
EBCDIC	Extended Binary Coded Decimal Interchange Code (Código Extendido de Intercambio Decimal Codificado en Forma Binaria).
EGP	Exterior Gateway Protocol (Protocolo para Gateway Exterior)
EOF	End of File (Fin del Archivo)

EOR	End of Record (Fin del Registro)
FCS	Frame Check Sequence (Secuencia de Verificación de Macos).
FDDI	Fiber Distributed Data Interface (Interfaz de Datos Distribuidos por fibra)
FIN	Final Segment (Segmento Final).
FTAM	Final Transfer, Access, and Management (Transferencia, Acceso y Administración de Archivos).
FTP	File Transfer Protocol (Protocolo para Transferencia de Archivos).
GGP	Gateway-to-Gateway Protocolo (Protocolo Gateway a Gateway).
GOSIP	Government Open System Interconnection Profile (Perfil de Interconexión para Sistemas Abierto de Gobierno).
GTF	Generalized Trace Facility (Medio de Rastreo Generalizado).
HDLC	High-Level Data Link Control Protocol (Protocolo de Control para Vinculo de Datos de Alto Nivel).
IAB	Internet Architecture Board (Comité de Arquitectura de Internet).
IAB	Internet Architecture Board (Comité de Arquitectura de Internet).
IAC	Interpret as Command (Interpretar como Comando).
IANA	Internet Assigned Numbers Authority (Autoridad Internet para Números Asignados).
ICMP	Internet Control Message Protocol (Protocolo Internet para Mensajes de Control).
ID	Identifier (Identificador)
IEEE	Institute of Electrical and Electronic Engineers (Instituto de Ingenieros Eléctricos y Electrónicos).
IEN	Internet Engineering Notes (Notas sobre Ingeniería Internet)
IESG	Internet Engineering Steering Group (Grupo Rector de la Ingenieria de Internet).
IGMP	Internet Group Management Protocol (Protocolo para Administración de Grupos Internet).
IGP	Interior Gateway Protocol (Protocolo para Gateway Interno).
IP	Internet Protocol (Protocolo de Internet).
IRTF	Internet Research Task Force (Brigada de Investigación en Internet).
ISDN	Integrated Service Digital Network (Red Digital de Servicios Integrados).
ISN	Initial Sequence Number (Número de Secuencia Inicial).
ISO	International Organization for Standardization
ISODE	ISO Development Enviroment (Ambiente de Desarrollo de la ISO).
LAN	Local Area Network (Red de Area Local).
LAPB	Link Access Procedures Balanced (Procedimientos Balanceados para Acceso al Vínculo).
LAPD	Link Access Procedures on the D-Channel (Procedimientos para Acceso el Vínculo en el Canal D).
LLC	Logical Link Control (Control Lógico del Vínculo).
MAC	Media Access Control (Control de Acceso al Medio).
MAN	Metropolitan Access Control (Control de Acceso al Medio)
MIB	Management Information Base (Base de Información sobre la Administración).

MSS	Maximum Segment Size (Tamaño Máximo del Segmento).
MTA	Message Transfer Agent (Agente para Transferencia de Mensaje).
MTU	Message Transfer Unit (Unidad para Transferencia de Mensajes).
MTU	Maximum Transmission Unit (Unidad para Trasmisión Máxima).
MX	Mail Exchanger (Intercambiador de Correspondencia).
NETBIOS	Network Basic Input/Output System (Sistema Básico de Entrada/Salida para Red).
NFS	Network File System (Sistema de Archivos de Red).
NIC	Network Interface Card (Tarjeta Interfaz de Red).
NIS	Network Infomation System (Sistema de Información de la Red).
NREN	National Research and Education Network (Red Nacional para la Investigación y la Educación).
NSAP	Network Service Access Point (Punto de Acceso al Servicio de la Red).
NSFNET	National Science Foundation Network (Red de la Fundación Nacional de Ciencias).
NVT	Network Virtual Terminal (Terminal Virtual de Red).
OSF	Open Software Foundation (Fundación Abierta para Software).
OSI	Open Systems Interconnection (Interconexión de Sistemas Abiertos).
OSPF	Open Shortest Path First (Abrir Primero la Ruta de Acceso Más Corta).
PAD	Packet Assembly/Disassembly (Montaje/Desmontaje de Paquetes).
PDU	Protocol Data Unit (Unidad para Datos del Protocolo).
PI	Protocolo Interpreter (Intérprete del Protocolo).
PING	Packet Internet Groper (Buscador Internet para Paquetes).
POP	Post Office Protocol (Protocolo para Oficina de Correos).
PPP	Point-to-Point Protocol (Protocolo Punto a Punto).
RARP	Reverse Address Resolution Protocol (Protocolo Inverso para Definición de Dirección).
RFC	Request for Comments (Peticiones para Comentarios).
RIPRPC	Routing Information Protocol (Protocolo de Información sobre el Enrutamiento).
RMONRST	Remote Network Monitor (Monitor de Red Remota).
RTT	Round Trip Time (Tiempo de Viaje Redondo).
SDLC	Synchronous Data Link Communication (Comunicación Sincrónica de Vínculo de Datos).
SLIP	Serial Line Internet Protocol (Protocolo Internet de Línea en Serie).
SMDS	Switched Multimegabit Data Service (Servicio Conmutado de Datos de Multimegabits).
SMTP	Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correspondencia).
SNA	Systems Network Architecture (Arquitectura de los Sistemas para Red).
SNMP	Simple Network Management Protocol (Protocolo Simple de Administración de Red).
SONET	Synchronous Optical Network (Red Óptica Sincrónica).
SPF	Shortest Path First (Primero la Ruta de Acceso Más Corta).

SSCP	Source Service Control Point (Punto de Acceso al Servicio de Fuente).
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
TCTCUP	Trunk Coupling Unit (Unidad de Acoplamiento Común).
TELNET	Terminal Networking (Redes Terminales).
TFTP	Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Archivos).
TLI	Transport Layer Interface (Interfaz de Capa de Transporte).
TP4	OSI Transport Class 4 (Clase 4 de Transporte de OSI).
TS4P	Transport Service Access Point (Punto de Acceso al Servicio de Transporte).
TTL	Time-to-Live (Tiempo de Vida).
UA	User Agent (Agente Usuario).
UDP	User Datagram Protocol (Protocolo de Datagrama de Usuario).
ULP	Upper Layer Protocol (Protocolo de Capa Superior).
WAN	Wide Area Network (Red de Área Amplia).
WDR	External Data Reperesentation (Representación de Datos Externos).
XNS	Xerox Networks Systems (Sistemas para Red Xerox).

ANEXO B

Para uso exclusivo del Instructor del laboratorio de Redes

En este anexo el instructor encontrara las disposiciones que deberá seguir en la práctica que se lo señale, ya que algunas de las prácticas requieren de instalación de software o configuración especial de los equipos antes de ser realizadas por los alumnos. Se seguirá el mismo orden cronológico de las prácticas y cabe aclarar nuevamente que algunas prácticas no requieren de acciones especiales antes de ser ejecutadas.

PRÁCTICA 2- CONFIGURACIÓN DEL PROTOCOLO TCP/IP

- Deberá de colocarse un icono de *"Entorno de Red"* en el escritorio de Windows.
- Las máquinas **No** deberán tener el protocolo de Internet configurado.
- Se deberá tener listos los datos que los alumnos utilizaran para configurar en sus respectivos equipos de trabajo el protocolo de Internet como son: DNS, direcciones IP, Mascara de subred, Puerta de enlace.
- En cuanto a las direcciones IP se deberá tener una lista con una dirección por equipo de trabajo.
- Los equipos beberán tener salida a Internet, así que cerciorese que la Red este funcionando adecuadamente.

Nota: En caso que el instructor decida realizar la práctica bajo Sistema Operativo Windows XP consulte la segunda parte del Anexo B donde se incluye la práctica elaborada y siga las mismas disposiciones para realizarla agregando esta última que se señala.

- Se deberá tener un icono de una conexión LAN nueva sin configurar.

PRÁCTICA 4 – MANEJO DE UN ANALIZADOR DE PROTOCOLOS (ETHEREAL)

- Deberá instalar previamente el software del analizador de protocolo de Ethereal (ir a la segunda parte del anexo B para instalación de Ethereal).
- Deberá colocarse un icono del programa Ethereal en el escritorio de Windows.
- Los equipos beberán tener salida a Internet o en Red Local, así que cerciorese que la Red este funcionando adecuadamente.

PRÁCTICA 5 – ANALISIS DE LOS PROTOCOLOS TCP E ICPM A TRAVÉS DE UNA ANALIZADOR DE PROTOCOLOS (ETHEREAL).

- Deberá instalar previamente el software del analizador de protocolo de Ethereal (ir a la segunda parte del anexo B para instalación de Ethereal).
- Deberá colocarse un icono del programa Ethereal en el escritorio de Windows.
- Los equipos beberán tener salida a Internet o en Red Local, así que cerciorese que la Red este funcionando adecuadamente.

Instalación del software Ethereal

Paso 1. Inserte el CD anexo a este trabajo que contiene el software de Ethereal en la unidad de CD-ROM.

Paso 2. Abra la carpeta llamada Ethereal.

Paso 3. Instale el software llamado WinPcap_3_0.exe necesario para que Ethereal pueda ser ejecutado dando doble clic en su respectivo icono de instalación.

Paso 4. Se abrirá una ventana de instalación, pulse el botón de *"Next"*.

Paso 5. De un clic en la opción *"Yes, Igree with all tems of thid license agreemente"* de otra forma no podrá ser instalado el software, una vez realizado este paso se activará el botón de *"Next"* de un clic sobre él para continuar con la instalación.

Paso 6. En la ventana siguiente vuelva a dar clic en el botón *"Next"* y por ultimo en la siguiente ventana presione el botón *"OK"*.

Paso 7. De doble clic en el icono de ethereal-setup-0.10.5a.exe

Paso 8. Una vez que aparezca la ventana de instalación de un clic en el botón *"Next"*.

Paso 9. En la siguiente ventana de un clic en el botón *"I Agree"*.

Paso 10. En la siguiente ventana en la opción *"Select the type of install:"* elija la opción *"Custom"* y de un clic en el botón de *"Next"*.

Paso 11. La siguiente ventana permite que elija la ubicación de instalación, ya no es necesario colocarla ya que la da automáticamente, de un clic en el botón de *"Install"*.Espere a que se instale el programa.

Paso 12. Por último de un clic en el botón *"Finish"*.

El software ha sido instalado y se encuentra listo para ser utilizado.

PRÁCTICA 3- CONFIGURACIÓN DEL PROTOCOLO TCP/IP
(Duración estimada: 60 minutos)

OBJETIVOS

- Que el alumno aprenda a configurar el protocolo de de comunicación TCP/IP.
+ Bajo ambiente gráfico Windows XP.
- Que el alumno realice pruebas para verificar que el equipo haya sido configurado correctamente.
- Que el alumno realice pruebas para comprobar que el equipo esta en buen estado y funcionando correctamente.

CUESTIONARIO PRELIMINAR

1. Explique brevemente los orígenes del protocolo de comunicación TCP/IP.
2. ¿Qué es la conmutación de paquetes?
3. ¿Qué es un paquete de información?
4. ¿Qué es un gateway?
5. ¿Qué son y para qué sirven las tablas de ruteo?
6. ¿A qué hace referencia el Loopback?
7. ¿Cuál es la dirección que identifica al gateway default y al loopback?
8. ¿Cuáles son las direcciones de equipo reservadas?
9. ¿Qué es y cómo funciona el algoritmo de encaminamiento?
10. ¿Qué es el direccionamiento físico y el direccionamiento lógico?
11. Define dirección estática y dirección dinámica.
12. Concepto de subred.

MARCO TEÓRICO

El protocolo de comunicaciones TCP/IP tiene sus orígenes en el proyecto de la agencia ARPA del gobierno de EUA para construir una red que funcionase con la tecnología de conmutación de paquetes allá por lo años 65, conocida como ARPAnet. Aparte de crear los dispositivos que permitieran la comunicación, se tenía que diseñar un protocolo que hiciera posible el intercambio de paquetes entre los equipos. Ello dio origen al primer protocolo utilizado de comunicación utilizado en ARPAnet, llamado NCP o Protocolo de Control de Red terminado para diciembre de 1970. Este protocolo no duró mucho, ya que tendía a actuar como un controlador de dispositivos y no como un conmutador de paquetes; por lo que en 1973 se empezó a desarrollar un nuevo protocolo denominado TCP (Protocolo de Control de Transmisión). Posteriormente sufrió modificaciones y dividió sus funciones en dos protocolos: TCP, encargado de las funciones de transporte, control de flujo y recuperación de paquetes, y el IP (Protocolo de Internet) encargado del direccionamiento de paquetes.

Posteriormente se incrementaría el protocolo ICMP para control de mensajes y retroalimentación de problemas., el protocolo UDP que brinda un acceso a IP para

aquellas aplicaciones que no requieran de los servicios de TCP, así como una gran variedad más de protocolos de aplicación (HTTP, FTP, Telnet, SMTP, etc.) y administración (SNMP, etc.) que enriquecen los servicios brindados. Es por ello que TCP/IP engloba a una gran cantidad de protocolos y no sólo TCP e IP.

Conmutación de paquetes

La red ARPAnet, y por ende Internet, opera bajo la tecnología de conmutación de paquetes; la cual consiste básicamente en lo siguiente: en un ambiente de redes, conocido comúnmente como *Internet* , que consiste de diversas redes que están enlazadas entre sí para formar una red más grande, se emplean dispositivos especiales que tiene la función de conmutar paquetes de una red a otra, de tal manera que puedan viajar de un equipo fuente a un equipo destino ubicado en otra red. Cuando un equipo tiene que enviar información a la red lo hace a través de paquetes; es decir, que la información a transmitir es dividida en pequeños pedacitos y a cada uno de estos se le añade información suficiente para que pueda viajar de forma independiente por las redes y llegar a su destino; a esto se le llama paquete.

Ruteo

Los dispositivos especiales que realizan la función como la conmutación de paquetes de red en red son los **ruteadores**, los cuales, tiene protocolos que les permiten generar diagramas completos de la estructura que tiene la red. Estos diagramas están en forma de tablas, conocidas como tablas de ruteo; estas, son consultadas por le protocolo IP que debe estar corriendo dentro del ruteador (en el caso de TCP/IP) para tomas las decisiones de cuál es el siguiente punto al que tiene que ser enviado un paquete para que llegue a su destino; es decir, que IP es el encargado de rutear los paquetes; por lo que el ruteo consiste en tomar las decisiones de cuál de todos los caminos posibles, es el que debe seguir un paquete para llegar a su destino, y una vez tomada la decisión, el paquete es liberado o enviado o enviado por dicho camino.

En la práctica, para unir las redes suelen ser empleados **Gateways**, los cuales, a demás de poder desempeñar las funciones de un ruteador, también puede cambiar de protocolos si es necesario.

En el caso de cualquier otro equipo (que no cuente con protocolos de ruteo), la tabla de ruteo se genera automáticamente al encender el equipo a través de la información que ha sido configurada cuando se instaló y configuró el protocolo TCP/IP, y se mantiene fija y sin ningún cambio durante su operación; a menos que se utilicen comando para modificarla manualmente por el usuario. Comparando las tablas de ruteo de los equipos contra las de los ruteadores, las primeras son generalmente más sencillas.

Las tablas de ruteo contienen entre otras cosas dentro de cada entrada, la dirección de una posible red destino y la dirección del ruteador (o gateway) al que tiene que ser enviado el paquete para que llegue a su destino.

Loopback es un nombre ya reconocido por los equipos e identifica al mismo equipo; es decir, que cuando se envía una señal al loopback el mensaje desciende por toda la pila de protocolos, y cuando IP detecta que el mensaje es para el loopback, lo envía de regreso ascendiendo nuevamente por la pila de protocolos hasta la aplicación. De ello se deduce que la señal nunca sale a la red; por lo que se utiliza para probar si el protocolo y demás dispositivos del equipo están funcionando correctamente (aunque el equipo no esté conectado a la red). En algunos sistemas, al *Loopback* suelen darle el nombre de "*Localhost*".

En términos generales, cuando un equipo desea enviar un paquete a un equipo destino se realiza un proceso conocido como "**algoritmo de encaminamiento**".

Direccionamiento

El direccionamiento permite localizar un objeto dentro de un grupo; para lo cual, se asigna una dirección única a cada objeto. En redes podemos clasificar el direccionamiento como: Físico y Lógico.

- El Direccionamiento Físico deriva su nombre del hecho de que estas direcciones son utilizadas en las capas inferiores del modelo OSI: Física y Enlace. Y por otro lado, porque a cada tarjeta d red que es construida, se le asigna una dirección única que es grabada en un circuito dentro de la tarjeta. Existe un organismo internacional encargado de administrar el banco d direcciones disponibles, y cada fabricante de tarjetas de red acude a ellos para solicitar que les sea asignado un banco de direcciones, para que ellos lo administren y puedan incorporar a cada tarjeta que construyen, una dirección de este tipo. Este mecanismo garantiza que dos tarjetas de red, independientemente de quien las fabrique, no tenga la misma dirección.
  A estas direcciones se les llama comúnmente "Direcciones Físicas" o "Direcciones MAC". Un ejemplo de dirección física es: 00-01-02-C9-8B-74.
  Una computadora tendrá una dirección física por cada tarjeta de red que posea.

- El Direccionamiento Lógico es empleado por el direccionamiento que se implementa a través de software; en el caso del direccionamiento numérico empleado por el protocolo IP, o el direccionamiento por nombres empleado por el protocolo DNS; ambos utilizados por TCP/IP en Internet.

  - ✓ Para el caso de IP se utilizan direcciones numéricas conocidas como "Direcciones IP". Estas se componen de 4 bytes que son representados en forma decimal, aislando cada byte por un punto; por ejemplo: 132.248.173.148. Una dirección IP permite identificar dentro de una gran red, como lo es la Internet, a cada equipo dentro de cada una de las redes que la conforman.
    Por otro lado, ya que TCP/IP es el protocolo oficial en Internet, se tiene que llevar un control sobre asignación de direcciones a los equipos u evitar que se dupliquen direcciones. Existe una organización que lleva el control

de las direcciones, y cuando una empresa desea conectarse a Internet, la organización le asigna un bloque de direcciones de a cuerdo a su tamaño. La empresa tiene la responsabilidad de asignar las direcciones IP a cada uno de sus equipos; siempre vigilando que no se repitan.

- ✓ El direccionamiento lógico es el de "nombres", como el empleado por el protocolo DNS (Domain Name System), que a continuación se describe:

  Una dirección por nombres está compuesta por varios nombres separados por un punto; por ejemplo: www.unam.mx

  Este tipo de direcciones surge por necesidad; ya que anteriormente se tenía que identificar a cada computadora en Internet por su dirección IP; lo cual, para nosotros los humanos resultaba u poco complicado al tener que recordar tantos números. Es por esa razón que surge este nuevo direccionamiento en Internet, por ejemplo: la UNAM, que es una institución mexicana, tiene un equipo que utiliza para darle el servicio de web a la comunidad universitaria y al público en general. A dicho equipo se le ha asignado el nombre de www.unam.mx, que es muy fácil de recordar en lugar de su dirección IP 132.248.10.7. el nombre completo del euipo está compuesto por el nombre del equipo (www) más el nombre del dominio al cual pertenece (unam.mx). El nombre del dominio puede estar compuesto por uno o más nombres de dominio; como en este caso, en el cual el dominio de la UNAM pertenece al dominio de mx (México). Otro ejemplo sería www.aragon.unam.mx indicando que el equipo www (servidor de web) pertenece al dominio de aragon (ENEP Aragón) el cual a su vez pertenece al dominio de la unam (UNAM) y este a su vez al dominio de mx (México).
  Al direccionamiento por nombres en esta modalidad se le conoce como direccionamiento por "nombres de dominio" y se implementa a través del protocolo de aplicación de TCP/IP llamado DNS. Básicamente DNS es una base de datos distribuida, a través e la cual, se puede hacer la conversión de direcciones IP a direcciones por nombres o viceversa. Cuando se utiliza este tipo de direccionamiento debe estar al alcance de cualquier equipo.
  Una persona puede asignar cualquier nombre a su computadora; pero si se requiere que ésta sea conocida a nivel mundial, dentro de la comunidad de Internet, el nombre del equipo debe ser registrado dentro de algún dominio, siguiendo los procedimientos establecidos y dentro de los cuales, se verifica que dicho nombre no se repita dentro del dominio. Una vez hecho esto, el nombre de la computadora estará compuesto por su nombre más el nombre del dominio en el cual fue registrado, separado por un punto.

Cuando se desea conectar una nueva computadora a una red, se le tiene que instalar el protocolo de comunicación al equipo y después configurarlo. En el caso de TCP/IP, para configurarlo se tienen que dar diversos parámetros y entre ellos se encuentran las

direcciones lógicas. Estos suelen ser asignados a los equipos de alguna de las dos siguientes formas:

- *De forma manual* dando estos parámetros durante el proceso de configuración, por lo que estos datos quedaran almacenados en algún archivo dentro del equipo. De esta forma, cada vez que equipo se encienda y arranque el software. Éste se configurará quedando siempre con los mismos datos; y entre ellos, la dirección lógica; que en el caso del Protocolo IP, es una dirección IP. Este parámetro no cambiará hasta que el usuario modifique y grabe los cambios en los archivos de configuración. A las direcciones lógicas que son asignadas de esta forma se les llama **direcciones estáticas.**

- *De forma automática.* en esta modalidad deberá existir algún mecanismo para que el equipo adquiera sus parámetros, y su dirección, de alguna forma automática. En el caso de TCP/IP nuevamente, se emplea el protocolo de aplicación llamado "DHCP". En este sistema, deberá existir en la red local donde se encuentra conectado el equipo, un servidor DHCP; el cual asigna de forma dinámica algunos parámetros a los equipos que lo soliciten (dirección IP, mascara de subred, etc.).

  Cuando un equipo se enciende, revisa sus archivos de configuración para establecer sus parámetros de funcionamiento; si se establece que debe obtenerlos automáticamente de la red, se utilizará el protocolo DHCP para enviar una señal al servidor DHCP solicitándoselos. Cuando el servidor recibe la petición, regresa una respuesta al equipo en la que se incluyen los parámetros, que han sido tomados de una base de datos que el servidor posee.

  El servidor DHCP lleva un control de los equipos que le han solicitado parámetros, así como la hora en que les han otorgado *(permiso obtenido)* y hasta cuando podrán ser usados *(permiso caduca)*.

  Cuando un permiso alcanza el tiempo establecido para poder utilizar estos valores *(permiso caduca)*, de manera automática envía una señal al servidor DHCP para pedir una renovación de tiempo, otorgándole un nuevo límite, hasta el cual, se podrán seguir utilizando los valores. Cuando el equipo es apagado, y por ,o tanto no renueva su tiepo, el servidor DHCP está en la posibilidad de asignar estos valores a otro equipo; es por ello que cada que se encienda el equipo, éste puede tener distintos valores. A este tipo de direcciones se les conoce como **direcciones dinámicas**; y nunca deben ser asignadas a equipos que fungirán como servidores.

HERRAMIENTAS Y RECURSOS

- 1 Equipo de cómputo con sistema operativo Windows 98 por cada grupo de trabajo.
- Conexión a Internet.
- Se pide al alumno los conocimientos suficientes para manejar S.O. Windows 98.
- Haber contestado el cuestionario preliminar.
  * El material se encuentra en el laboratorio.

DESARROLLO

Explicación: el alumno llevará un registro (donde se le indique) de los eventos que se vayan desarrollando para posteriormente entregar un reporte con los siguientes criterios:

- Los pasos de mayor grado de dificultad al realizar la práctica.
- Problemas encontrados al realizar la práctica.
- Observaciones
- Resultados obtenidos al realizar las pruebas.
- Respuestas a las preguntas que se realicen a lo largo de la práctica.

PARTE DE CONFIGURACIÓN DEL PROTOCOLO TCP/IP

Paso 1. Encienda el equipo que le haya sido asignado.

Paso 2. Cuando aparezca la ventana de *"Contraseña de Red"*, accese al ambiente Windows digitando en *"Nombre de Usuario"* el nombre de la PC y en el de *"Contraseña"* vuelva a escribir el nombre de la PC. Por ultimo de un clic en botón de *"Aceptar"* o presione la tecla de *"Enter"*.

Paso 3. Clic en el botón de *"Inicio"*.

Paso 4. Clic en la opción *"Panel de Control"*.

Paso 5. Clic en el icono de *"Conexiones de Red"* en esta ventana se encuentra una conexión y será la que se configure.

Paso 6. Clic derecho de Mouse sobre el icono de la conexión y de un clic en la opción *"Propiedades"*.

Paso 7. De la ventana de *"Propiedades de Conexión"* seleccionar de la parte donde se listan los elementos de la red la opción del *"Protocolo de Internet (TCP/IP)"* y dar un clic sobre él, posteriormente dar clic en el botón de *"Propiedades"*.

Paso 8. A continuación en la ventana de *"Propiedades de Protocolo de Internet (TCP/IP)"* elija la pestaña de *"General"*.

Paso 9. De un clic en la opción *"Usar la siguiente dirección IP:"*, una vez que se de clic en esta opción se habilitaran los campos *"Dirección IP"*, *"Mascara de subred"* y *"Puerta de enlace predeterminada"*.

Paso 10. Llenar cada uno de los campos antes mencionados *Dirección IP"*, *"Mascara de subred"* y *"Puerta de enlace predeterminada"* con los datos que su instructor le proporcione.

Paso 11. En esa misma ventana mas abajote un clic en la opción *"Usar las siguientes direcciones de servidor DNS:"* una vez que se de clic en esta opción se habilitaran los campos *"Servidor DNS preferido"* y *"Servidor DNS alternativo"*.

Paso 12. Llene cada uno de los campos antes mencionados *"Servidor DNS preferido"* y *"Servidor DNS alternativo"* con los datos que su instructor le proporcione.

Paso 13. Por ultimo de un clic en el botón de *"Aceptar"*.

Nota: la pestaña *"Configuración alternativa"* se utiliza en el caso de que el equipo se utilice en más de una red.

PARTE DE COMPROBACIÓN DE LA CONFIGURACIÓN

Paso 14. Para comprobar que el equipo se encuentra configurado correctamente y tiene acceso a la red, ejecute una ventana del *"Internet Explorer"* y en el campo de *"dirección"* escriba *"http://www.unam.mx* . Al realizar este paso debe establecerse conexión con el servidor web de la UNAM y se deberá desplegar su página en la pantalla. De lo contrario pida apoyo a su asesor para localizar la falla. Si se desplegó la pagina, cierre la ventana del *"Internet Explorer"* y siga con el siguiente paso de la práctica.

Paso 15. Abra una ventana de *"MS-DOS"* dando clic en el menú *"Inicio"* y seleccionando la opción *"Ejecutar"* a continuación escriba *command* en el campo y por ultimo de un clic en el botón de *"Aceptar"* o presione tecla de *"Enter"*.

Paso 16. En el prompt de *"MS-DOS"* ejecute el comando:
C:\WINDOWS>IPCONFIG

Paso 17. Anote los parámetros que correspondan a su tarjeta de red de:

Dirección IP: _____
Máscara de Subred: _____
Puerta de enlace predeterminada: _____

Paso 18. En el prompt de *"MS-DOS"* ejecute el comando:
C:\WINDOWS>IPCONFIG /all | more

Como se puede observar, en la pantalla sale información que se encuentra dividida en dos partes: *"Configuración IP de Windows 98"* y *"0 Ethernet adaptador"*. De la primera, los parámetros que nos interesan para esta práctica son, el *"Nombre del Host"*, y el *"Servidor de DNS"*, en el cual se establece la dirección numérica del equipo servidor DNS.

En la segunda parte *"0 Ethernet adaptador"*, los parámetros que nos interesan son: la *"Dirección Física"*, que se refiere a la dirección que tiene grabada físicamente la tarjeta de red 0, para este caso. El de *"DHCP activado"*, que básicamente indica si este protocolo se encuentra activado y que al estarlo los parámetros se asignaran de forma dinámica.; así como los parámetros de *"Permiso obtenido"* y *"Permiso caduca"*, que se encargan de establecer la vigencia del derecho a usarlos. Los de *"Servidor WINS primario"* y *"Servidor WINS secundario"*, que se encargan de determinar si es que se esta utilizando un servidor WINS que se encuentre dentro de la red local, en último lugar, los parámetros de *"Dirección IP"*, *"Mascara de red"* y *"Puerta de Enlace Predeterminada"*, que deben coincidir con los datos obtenidos en el paso 17 y por supuesto con los que fueron asignados por el asesor.

Anote cada uno de los parámetros establecidos en este punto.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____.

Paso 19. De los conocimientos adquiridos en el paso anterior conteste las siguientes preguntas:

- ✓ ¿De qué forma se encuentra establecida la dirección IP del equipo?

_____

- ✓ ¿A qué dominio pertenece su equipo?

_____

- ✓ ¿Se encuentra activado algún servidor WINS?

_____

✓ El parámetro de "*permiso caduca*" ¿tiene algún valor establecido?

✓ En caso negativo, ¿qué significa eso?

✓ ¿Qué función tiene la opción "Obtener una dirección IP automáticamente?

Nota: Todos los datos obtenido en el paso17 tienen que coincidir con los datos que su asesor le proporciono para configurar su equipo con el protocolo TCP/IP, si es así paso al paso siguiente de lo contrario pregunte a su asesor y verifiquen la posible falla.

CONCLUSIONES

Que el alumno haga un análisis de cada uno de los pasos que llevo a cabo y comente dudas y haga aclaraciones de todo lo que pudo aprender en esta práctica.

ANEXO C

Encuestas, estadísticas y gráficas.

Se tomaron como referencia 6 preguntas totalmente enfocadas a la materia de Redes de computadoras y fueron las mismas para profesores, alumnos y exalumnos ver Anexo C.

Como primer punto se analizaron los cuestionarios de los profesores.

Formato de encuesta profesores

1. ¿Cree que son necesarias las prácticas del laboratorio? ¿Por qué?.
2. ¿Le parece que hagan falta laboratorios para alguna materia?
3. Si su respuesta a la pregunta anterior fue si ¿Para qué materias cree que haga falta un laboratorio?
4. ¿Le parece buena la idea de implementar un laboratorio para materia de Redes de Computadoras? ¿Por qué?
5. Tomando en cuenta que se implementara un laboratorio para la materia de Redes de Computadoras, esto implicaría 2 horas más de tu tiempo de estudio, ¿estaría dispuesto a impartir el laboratorio? ¿Por qué?
6. ¿Cuál sería su aportación para la implementación de este laboratorio?
7. ¿De qué forma cree que influyan los laboratorios en la formación profesional?

A continuación se transcriben los cuestionarios aplicados a los profesores y por respeto a los profesores se omitieron sus nombres.

1. ¿Cree que son necesarias las prácticas del laboratorio? ¿Por qué?

R= Si, porque complementa el aprendizaje teórico de los conceptos teóricos.

2. ¿Le parece que hagan falta laboratorios para alguna materia?
R= Si
3. Si su respuesta a la pregunta anterior fue si ¿Para qué materias cree que haga falta un laboratorio?
R= De la materia de Redes de Computadoras.

4. ¿Le parece buena la idea de implementar un laboratorio para materia de Redes de Computadoras? ¿Por qué?
R= Indispensable para la formación de los alumnos.

5. Tomando en cuenta que se implementara un laboratorio para la materia de Redes de Computadoras, esto implicaría 2 horas más de tu tiempo de estudio, ¿estaría dispuesto a impartir el laboratorio? ¿Por qué?
R= Si, porque contribuye a la creación de esta herramienta fundamental para el aprendizaje.

6. ¿Cuál sería su aportación para la implementación de este laboratorio?
R= Redacción de la práctica como documento pase o guía para la ejecución con los equipos involucrados.

7. ¿De qué forma cree que influyan los laboratorios en la formación profesional?
R= Totalmente, dado que desarrollan las habilidades y competencia que el alumno debe poseer.

1. ¿Cree que son necesarias las prácticas del laboratorio? ¿Por qué?
R= Si, para una vinculación entre la teoría y la práctica.

2. ¿Le parece que hagan falta laboratorios para alguna materia?
R= Si.

3. Si su respuesta a la pregunta anterior fue si ¿Para qué materias cree que haga falta un laboratorio?
R= Redes de computadoras

4. ¿Qué opina acerca de implementar un laboratorio para materia de Redes de Computadoras? ¿Por qué?
R= Opino que es muy necesario ya que es muy importante esta materia para la formación del ingeniero en computación.

5. Tomando en cuenta que se implementara un laboratorio para la materia de Redes de Computadoras, esto implicaría 2 horas más de tu tiempo de estudio, ¿estaría dispuesto a impartir el laboratorio? ¿Por qué?

R= No, ya no cuento con el tiempo necesario.

6. ¿Cuál sería su aportación para la implementación de este laboratorio?
R= La que la coordinación pretenda en pedir ayuda.

7. ¿De qué forma cree que influyan los laboratorios en la formación profesional?
R= D e una forma muy grande.

1. ¿Cree que son necesarias las prácticas del laboratorio? ¿Por qué?
R= Si, ya que brinda una forma de comprobar y poner en práctica los conocimientos teóricos adquiridos durante las clases, además de dotar de habilidades en el manejo de hardware y software específicos de la materia

2. ¿Le parece que hagan falta laboratorios para alguna materia?
R=Si

3. Si su respuesta a la pregunta anterior fue si ¿Para qué materias cree que haga falta un laboratorio?
R= Comunicaciones digitales, Redes de computadoras entre otras

4. ¿Qué opina acerca de implementar un laboratorio para materia de Redes de Computadoras? ¿Por qué?
R= Excelente.

5. Tomando en cuenta que se implementara un laboratorio para la materia de Redes de Computadoras, esto implicaría 2 horas más de tu tiempo de estudio, ¿estaría dispuesto a impartir el laboratorio? ¿Por qué?
R= Si, como docente me permite estar satisfecho con mi trabajo y brindar la posibilidad de que los alumnos adquieran mayores conocimientos que les permitan hacer frente a las mayores demandas del mercado laboral.

6. ¿Cuál sería su aportación para la implementación de este laboratorio?
R= Mis conocimientos, experiencia y disposición para la creación del laboratorio.

7. ¿De qué forma cree que influyan los laboratorios en la formación profesional?
R= Dotándolos de experiencia, conocimientos y habilidades.

1. ¿Cree que son necesarias las prácticas del laboratorio? ¿Por qué?
R= Si, porque debe existir una parte práctica del temario.

2. ¿Le parece que hagan falta laboratorios para alguna materia?

R= Si.

3. Si su respuesta a la pregunta anterior fue si ¿Para qué materias cree que haga falta un laboratorio?

R= Las que correspondan al área de sistemas.

4. ¿Qué opina acerca de implementar un laboratorio para materia de Redes de Computadoras? ¿Por qué?

R= Buena decisión. ¿Cómo?, ¿dónde?, ¿Con qué?, ¿Quiénes?

5. Tomando en cuenta que se implementara un laboratorio para la materia de Redes de Computadoras, esto implicaría 2 horas más de tu tiempo de estudio, ¿estaría dispuesto a impartir el laboratorio? ¿Por qué?

R= Si, como valor agregado

6. ¿Cuál sería su aportación para la implementación de este laboratorio?

R= La logística, puesta a punto y operación.

7. ¿De qué forma cree que influyan los laboratorios en la formación profesional?

R= Como experiencia profesional.

Formato de encuesta alumnos

1. ¿Crees que son necesarias las prácticas del laboratorio? ¿Por qué?
2. ¿Te parece que hagan falta laboratorios para alguna materia?
3. Si tu respuesta a la pregunta anterior fue si ¿Para qué materias crees que haga falta un laboratorio?
4. ¿Te parece buena la idea de implementar un laboratorio para materia de Redes de Computadoras? ¿Por qué?
5. Tomando en cuenta que se implementara un laboratorio para la materia de Redes de Computadoras, esto implicaría 2 horas más de tu tiempo de estudio, ¿estarías dispuesto a impartir el laboratorio?¿Por qué?
6. ¿cuál sería tu aportación para la implementación de este laboratorio?
7. ¿De qué forma crees que influyan los laboratorios en la formación profesional?

A continuación se muestran los resultados obtenidos de las encuestas aplicadas a los alumnos que cursan actualmente la materia de Redes de Computadoras. Se manejo un estándar de respuestas y se trabajo con las más relevantes o importantes para los alumnos.

1- ¿Crees que son necesarias las practicas de laboratorio?

Si	95% (48 encuestas)
Porque? (Principales observaciones)	Para reafirmar los conocimientos de la teoria. Facilitar el manejo de los equipos. Porque es parte integral de la formación como ingenieros.
NO	5% (2 encuestas)
Porque? (Principales observaciones)	Algunas materias con laboratorio no son comunes en el campo laboral.

2- ¿Te parece que hagan falta laboratorios para algunas materias?

Si	95% (48 encuestas)	No	5% (2 encuestas)

3- ¿Para que materias crees que haga falta un laboratorio?

Redes, Programación estructurada, Sistemas operativos, Ingenieria de programación, Robotica.

4- ¿Te parece buena la idea de implementar un laboratorio para la materia de redes de computadoras?

Si	100% (50 encuestas)
Porque? (Principales observaciones)	Es una materia que necesita practica, puesto que es hardware. Con un laboratorio se aprende y se practica la instalación y reparación de las redes. Se solucionan los problemas que se pueden presentar en forma fisica
NO	0% (0 encuestas)
Porque? (Principales observaciones)	

5- Tomando en cuenta que se implementara un laboratorio para la materia de redes de computadoras esto implicaria dos horas mas de tu tiempo de estudio ¿estarias dispuesto a cursarlo?

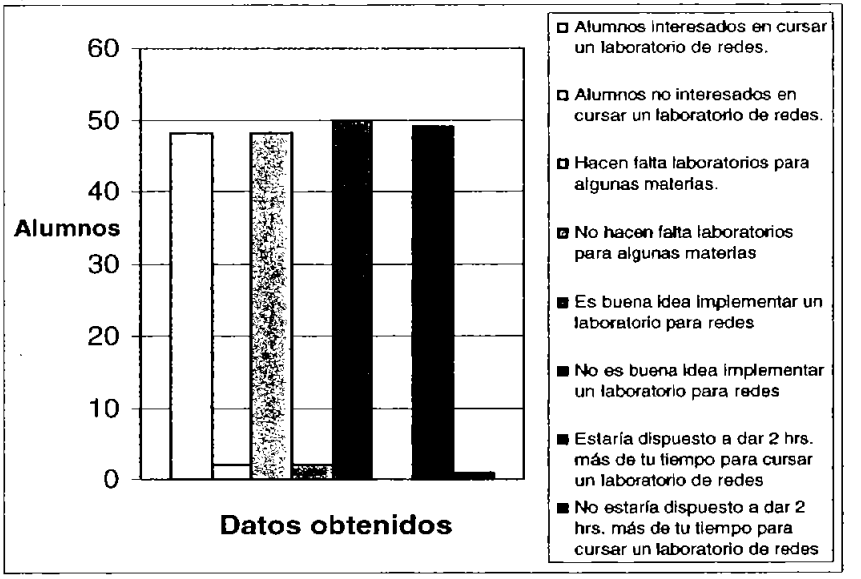
Si	97% (49 encuestas)
Porque? (Principales observaciones)	Seria un tiempo invertido en nuestra formación profesional. Aunque uno no se dedique a esa area, serviria de conocimientos generales.
NO	3% (1 encuesta)
Porque? (Principales observaciones)	Seria mejor distribuir las horas totales de la teoria con la practica.

6- ¿Cual seria tu aportaciòn para la implementación de este laboratorio?

COMENTARIOS Con aportación de material y la difusión de los conocimientos a las proximas generaciones.

7- ¿De que forma crees que influyan los laboratorios en la formación profesional?

COMENTARIOS Los laboratorios ayudan a conocer de forma real efectos, causas, etc., de algunos temas. Son como una pequeña prueba de la vida profesional que ejerceremos.



Grafica 1. Resultados obtenidos de las encuestas realizadas

	ANIEI	INSTITUTO POLITECNICO NACIONAL	ITESM Campus Cd. De México	UNAM ENEP Aragón	UNIVERSIDAD DEL VALLE DE MEXICO
TEMAS	SUBTEMAS	TEMAS	TEMAS	TEMAS	TEMAS
Conceptos	Transmisión y comunicación de información	Transmisión y comunicación de datos	Modelo de comunicación de datos.		Modelo de comunicación de datos.
Códigos	BCD, ASCII, EBCDIC		Introducción a la Informática (Materia de otro semestre)	Codigo de entrada y salida.	Introducción a la Informática (Materia de otro semestre)
Errores	Deteccion y Correccion de Errores Algoritmos: Paridad, sumas de verificacion , CRC.	Métodos de detección y corrección de errores.	Autentificación. Control de congestión.	Detección y corrección de errores. Modulacion por pulsos codificados (PCM)	Autentificación. Control de congestión.
Señales, tipos y enlaces	Moderns. Señales Analogicas y Digitales. Modulación y Demodulación: AM, FM y PM.	Transmisión de datos digital y analógica.	Señalización digital y analógica.	Elementos de hardware: módems	Señalización digital y analógica.
Comunicaciones	Circuitos Dedicados y Circuitos No Dedicados Conmutación de circuitos y paquetes. Espectro de frecuencia, Ancho de Banda Velocidad de canal, capacidad de transmisión.	Transmisión y Conmutación de datos	Servicios orientados a conexión y no -conexión Técnicas de Conmutación.	Conmutación de circuitos, mensajes y paquetes.	Servicios orientados a conexión y no -conexión Técnicas de Conmutación.
Modos de transmision	Transmisión Síncrona y Asíncrona Multiplexaje por división de frecuencias y de tiempos Métodos de transmisión en serie y paralelo.		Comunicación de datos. Multiplexo. Comunicación de datos.	Comunicación síncrona binaria. Multiplexaje por división de tiempo (TDM)	Comunicación de datos. Multiplexo. Comunicación de datos.
Medios y elementos físicos	Coaxial, Par trenzado, Fibra Óptica, Satélite, Microondas. Redes Publicas Digitales, Redes Telefonicas.	Medios Físicos de transmisión de datos.	Medios de transmisión.	Medios físicos de transmisión.	Medios de transmisión.
Servicios de comunicaciones	Video Interactivo, Videoconferencia, teleconferencia. Estándar ITU H.320. ISDN		ISDN.	Redes de servicios integrados.	ISDN.
Modelo OSI	Capas del modelo OSI/ISO.	El Modelo de referencia de interconexión de sistemas abiertos.	Modelo OSI.	Modelos principales de arquitectura de redes: Modelo OSI	Modelo OSI.
Estándares y Organizaciones	IEEE, ITU, OSI, SNA, DNA, SNA.		Estándares.		Estándares.
Redes locales LAN	Elementos de una red LAN (Tarjeta de red, Cableado, Software). Topologías Físicas. Protocolo CSMA/CD, Token Passing. Estándares IEEE 802.3, IEEE 802.4, IEEE 802.5 Sistemas Operativos de Red.	Redes de Área Local. Protocolos de comunicación para LAN's. Protocolos de comunicación del estándar 802 de IEEE.	Cableado Estructurado. Topologías. Control de Acceso al Medio. Estándares.	Redes de Área Local, cobertura geográfica. Procedimientos de acceso al canal de datos	Cableado Estructurado. Topologías. Control de Acceso al Medio. Estándares.

	ANIEI	INSTITUTO POLITECNICO NACIONAL	ITESM Campus Cd. De México	UNAM ENEP Aragón	UNIVERSIDAD DEL VALLE DE MEXICO
TEMAS	SUBTEMAS	TEMAS	TEMAS	TEMAS	TEMAS
Redes de área amplia WAN	Dispositivos DTE y DCE. ATM, X.25, Frame Relay. Conexiones de punto a punto y punto-multipunto. Aplicaciones: Consultas compartidas, terminal virtual.	Protocolo de transporte sencillo sobre el estándar X.25	ATM, Frame Relay. Diseño de Redes LAN y WAN.	Norma X.25 No incluye tecnologías superiores. Tipos de enlaces básicos: Punto a Punto, multipunto.	ATM, Frame Relay. Diseño de Redes LAN y WAN.
Protocolos de bajo nivel	Protocolos de capa física: RS-232, RS449. Protocolos Orientados a caracteres y a bits: ISO/HDLC. Protocolos de capa de red X.25, IP, Frame Relay, ATM. Direcciones IP.	Transmisión y comunicación de datos capa física. Protocolos elementales de la capa de enlace de datos. Aspectos generales de la capa de red. TCP/IP	Comunicación de datos.	Elementos de Hardware: RS-232, RS439. Manejo de protocolo HDLC. Solo X.25 Solo a nivel general " Protocolo TCP/IP"	Comunicación de datos.
Protocolos de alto nivel	Protocolos de capa de transporte: TCP, UDP, IPX, Apple Talk. Protocolos de la capa de sesion: X.215 Protocolos de la capa de presentación: ASN.1, X.409 Protocolos de la capa de aplicación: X.400 y X.500	Aspectos generales de la capa de transporte. Aspectos generales de las capas de usuario. Aspectos generales de las capas de usuario.	TCP/IP y SNA. Servicios de la capa de sesión Servicios de la capa de presentación		TCP/IP y SNA. Servicios de la capa de sesión Servicios de la capa de presentación
Redes interconectadas	Programación de Sockets. Teoría de enrutamiento. Protocolos para la resolución de direcciones ARP, RARP. Subredes y Mascaras. Dominio Unix.	Sockets. Algoritmos de enrutamiento de datos. TCP/IP TCP/IP	Protocolos de enrutamiento.	Solo a nivel general " Protocolo TCP/IP"	Protocolos de enrutamiento.
Dispositivos	Repetidores, Hubs, Switches, Puentes, Gateways, Enrutadores.		Diseño de Redes LAN y WAN.		Diseño de Redes LAN y WAN.
Optimización de redes	Optimización de redes, costos,servicios, tráfico.		Desempeño de redes.		Desempeño de redes.
Administración de redes	Administración y Supervisión.		Administración de una red.	Programas para la administración de la red.	Administración de una red.
Internet	World Wide Web, HTML y creación de scripts. Ipv6. Servicio de nombres DNS. Transferencia remota de archivos y correo electrónico.		Aplicaciones de red HTTP.		Aplicaciones de red HTTP.
Seguridad	Criptografía. Firewall. Comunicación confiable entre aplicaciones: traps.	Comunicación entre procesos.	Seguridad en redes.		Seguridad en redes.

Glosario

A continuación se presentan algunos términos que se pueden encontrar a lo largo del presente trabajo:

10Base2 Un término de Ethernet que representa una velocidad de transmisión máxima de 10 Mega bits por segundo y que utiliza una señalización de banda de base, con una longitud continúa para el segmento del cable de 100 metros y un máximo de dos segmentos.
10Base5 Un término de Ethernet que representa una velocidad de transmisión máxima de 10 Mega bits por segundo y que utiliza una señalización de banda base, con 5 segmentos continuos que no exceden los 100 metros por segmento.
10BaseT Un termino de Ethernet que representa una velocidad de transmisión máxima de 10 Mega bits por segundo y que utiliza una señalización de banda base y un cable dúplex.
Abrir Primero la Ruta de Acceso Mas Corta, OSPF (Open Shortest Path First). El protocolo básico para enrutamiento en Internet, utilizado para enviar datos por varias rutas de acceso. Utiliza la topología de la red para enlutar las decisiones.
Acceso Múltiple de Detección de Aportación con Detección de Colisión, CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Un protocolo de control de acceso para medios de red donde un dispositivo escucha al medio para vigilar el tráfico. Si no existe ninguna señal, el dispositivo puede enviar la información.
Acknowledgment, ACK (Acuse de recibo). Una respuesta positiva que regresa un receptor hacia el remitente, indicándole que la conexión tuvo éxito. TCP utiliza los acuses de recibo para indicar la recepción exitosa de un paquete.
Administración de la red. Cualquiera de los aspectos de la vigilancia o el control de una red, incluyendo todos los detalles administrativos.
Advanced Research Project Agency, ARPA (Agencia de proyectos de Investigación Avanzada). El nombre anterior de DARPA. ARPA era una agencia que fundó el gobierno federal de los EU., en un principio exclusivamente para la investigación. Cuando cambió a DARPA, los fondos pasaron a ser parte del presupuesto de defensa.
Agente. En TCP/IP, un agente es un proceso SNMP que responde a las solicitudes get y set. Los agentes también pueden enviar mensajes desviados.
Agente usuario (User Agent) Un programa de correo electrónico que ayuda a los usuarios finales a administrar sus mensajes.
American Nacional Standards Institute, ANSI (Instituto Nacional de Normas de Estados Unidos). El organismo norteamericano responsable de fijar las normas.
Ancho de Banda. El alcance de frecuencias que se transmiten en un canal, o la diferencia entre la frecuencia más alta y la más baja transmitidas a través de un canal.
Apertura Activa. Una operación que realiza un cliente con el fin de establecer una conexión TCP con un servidor.
Apertura Pasiva. Una acción tomada por un daemon servidor para prepararse a recibir las solicitudes de los clientes.

ARPANET (Advanced Research Projects Agency Network) (Red de la Agencia de Proyectos de Investigación Avanzada) Una red de conmutación de paquetes que posteriormente se conoció como Internet.

Arquitectura cliente/servidor. Un término generalizado que se utiliza para hacer referencia a un ambiente distribuido, en el cual un programa puede iniciar una sesión y otro puede responder a sus solicitudes. El origen de los diseños cliente/servidor esta estrechamente ligado con la suite del protocolo TCP/IP.

ASCII (American Nacional Standard Code for Information Interchange) (Código Estándar Americano para Intercambio de Información) Un conjunto de caracteres de 8 bits que define a los caracteres alfanuméricos.

Asíncrono. Cuando las comunicaciones no cuentan con una base de tiempo regular, y permiten las transmisiones a velocidades desiguales.

Banda ancha (también conocida como banda amplia) Un alcance de frecuencias que está dividido en varias bandas más angostas. Cada banda puede utilizarse para distintos propósitos.

Banda de base. Un tipo de canal en donde la transmisión de datos se conduce a través de un solo canal de telecomunicaciones, y que soporta solamente una transmisión de señal a la vez. Ethernet es un sistema de banda de base.

Base de Información sobre Administración, MIB (Management Information Base) Una base de datos utilizada por SNMP que contiene la información sobre la configuración y la información estadística acerca de los dispositivos que se encuentran en una red.

Brouter (Enrutador de puente) Un dispositivo para red que es una combinación de las funciones de un puente y un enrutador. Puede funcionar como un puente mientras filtra los protocolos y los paquetes que están destinados para los nodos de diferentes redes.

Búfer (Buffer) Un área de la memoria que se utiliza para manejar la entrada (input) y la salida (output).

Bus. En la topología de una red es una configuración lineal. También se utiliza para referirse a parte de la disposición electrónica de los dispositivos para red.

Caché. Una ubicación de la memoria que tiene listo la materia que se solicita constantemente. Por lo general, el caché es mas rápido que el dispositivo de almacenamiento. Se utiliza para acelerar la transferencia de datos y de instrucciones.

Capa de aplicación. La capa más alta del modelo OSF. Establece los derechos de las comunicaciones y puede iniciar una conexión entre dos aplicaciones.

Centro de Información para la Red, NIC (Network Information Center). Medio proporcionado por la administración de Internet que controla los nombres de las redes que son accesibles en Internet.

Clase 4 de transmisión (Transmisión Class 4) Un protocolo OSI para capa de transporte que es similar al TCP. En ocasiones se le conoce como OSI TP4.

Cliente. Un programa que intenta conectarse a otro programa (generalmente en otra maquina) llamado servidor. El cliente llama al servidor. El servidor escucha las llamadas.

Colisión. Un evento que ocurre cuando dos o más nodos transmiten paquetes al mismo tiempo; es decir cuando los paquetes chocan.

Columna vertebral (Backbone). Un conjunto de nodos y vínculos conectados y que comprenden una red, o los protocolos de la capa superior utilizados en una red. Algunas veces, el término se utiliza para hacer referencia al medio físico de una red.

Conexión. Un vinculo entre 2 o mas procesos, aplicaciones, máquinas, redes, etc. Las conexiones pueden ser lógicas, fisicas o de ambos tipos.
Conexión conmutada (Switched Connection) Una conexión para vinculo de datos que se establece por demanda (como una llamada telefónica).
Contador de Saltos (Hop Count) El número de puentes por los que atraviesa la información en una red Token Ring.
Contención. Una condición que ocurre en algunas LAN en donde la subcapa de Control de Acceso al Medio (MAC) permite que más de un nodo pueda hacer una transmisión al mismo tiempo, aumentando el riesgo de que existan colisiones.
Control de Acceso. Un proceso que define los privilegios que tiene cada usuario en el sistema.
Control de Acceso al Medio MAC (Media Access Control) La mitad inferior de la subcapa para vinculo de datos que es responsable de enmarcar los datos y controlar el vinculo fisico entre dos puntos terminales.
Control de Vínculos Lógicos LLC (Logical Link Control) La parte superior del protocolo para subcapa de vínculo de datos que es responsable de regir el intercambio de datos entre dos puntos terminales.
Control para Vínculo de Datos de Alto Nivel, HDLC (High Level Data Link Control) Un estándar internacional para comunicación de datos.
Conversión de protocolo. El proceso de cambiar de un protocolo a otro.
Crosstalk (Diafonía) Las señales que interfieren con otra señal.
DARPA, Agencia de Proyectos de Investigación Avanzada de la Defensa (Defense Advanced Research Project Agency) El organismo gubernamental que creó DARPANET para comunicaciones de gran extensión. DARPANET posteriormente se convirtió en Internet.
Datagrama. Una unidad básica de información utilizada con TCP/IP.
Datagrama IP. La unidad básica de información que se transmite a través de una red TCP/IP. La cabecera del datagrama contiene las direcciones IP de origen y destino.
Definición de dirección. El mapeo de una dirección IP para la dirección física de una maquina. TCP/IP utiliza el Protocolo para Definición de Dirección (ARP) para esta función.
Definición de nombre (Name Resolution) El proceso de mapeo de los alias de una dirección. El servicio de Nombre de Dominio (DNS) es un sistema que lleva acabo esto.
Definidor (Resolver) El software que permite a los clientes tener acceso a la base de datos del Servicio para Nombre de Dominio (DNS) y adquirir una dirección.
Descriptor de conector (Socket Descriptor) Un Número entero utilizado por una aplicación para identificar la conexión.
Detección de Colisión. La capacidad que tiene un dispositivo de detectar cuando ha ocurrido una colisión.
Detección de portación. (Carrier Sense) Una señal que genera la capa física de la red, para informar a la capa de vinculación de datos que uno o más nodos está llevando a cabo transmisiones por medio de la red.
Dirección. Una sección de la memoria que se encuentra dentro del RAM de una máquina en particular. Un identificador numérico o un nombre simbólico que especifica la colocación de una máquina o dispositivo específicos dentro de una red, y un medio de identificar a toda una red, a una subred o a un nodo que se encuentran dentro de una red.

Dirección de destino (Destination Address) La dirección del dispositivo final al que van destinados los datos.
Dirección de Hardware. LA dirección de bajo nivel asociada con cada dispositivo que se encuentra en una red, generalmente correspóndela identificador exclusivo de la tarjeta interfaz para red (NIC). Las direcciones de Ethernet son de 48 bits.
Dirección de Red. En TCP/IP la dirección de 32 bits de un dispositivo.
Dirección de subred. La parte de la dirección IP que identifica la subred.
Dirección Ethernet. Una dirección de 48 bits conocida comúnmente como dirección física o dura, que únicamente identifica la Tarjeta Interfaz para Red Ethernet (NIC), así como el dispositivo donde reside la tarjeta.
Dirección Internet. Una dirección de 32 bits que se utiliza para identificar a los hosts y a las redes que están en Internet.
Dirección IP. Un identificador de 32 bits que es único para cada dispositivo de la red.
Dirección Socket (Socket Address) La designación completa de un nodo TCP/IP que consta de una dirección IP de 32 bits y un número de puerto de 16 bits.
Emisión (Broadcast). La Transmisión simultanea de los mismos datos hacia todos los nodos que están conectados a la red.
Encapsulación. Cuando se incluye un mensaje de entrada dentro de otro más extenso, agregando información al frente, atrás, o en ambas partes del mensaje. La encapsulación la utilizan los protocolos para redes en capas. Con cada capa se agregan nuevos encabezados (headers) y colas (trailers).
Enrutador. Un dispositivo que conecta a las LAN dentro de una red interna y que dirige el tráfico entre ellas.
Enrutamiento. El proceso de determinar la ruta de acceso a utilizar para enviar los datos a su destino.
Ethernet. Un protocolo a nivel de vínculo de datos que comprende las dos capas inferiores del modelo OSI. Es una tecnología para transmisión de redes que puede utilizar varios medios físicos diferentes, incluyendo cable dúplex y cable coaxial. Ethernet generalmente utiliza CSMA/CD. TCP/IP comúnmente lo utilizan las redes ethernet.
Fibra óptica. Un cable de plástico o vidrio que utiliza la luz como medio para las comunicaciones.
Fragmentación. La división de un datagrama en varias piezas más pequeñas, generalmente debido a que el datagrama original era demasiado extenso para la red o para el software.
Gateway. En términos de Internet, un gateway es un dispositivo que enruta los datagramas. Más recientemente utilizado para hacer referencia a cualquier dispositivo de red que traduce los protocolos de un tipo de red a los de otra red.
Gigabyte. Mil millones de bytes, correspondiente al numero decimal, 1,073,741,824 (un kilobyte equivales al decimal 1,024).
IEEE 802.3 Un estándar para capa física aprobado por el IEEE que utiliza CSMA/CD en una topología para red de bus.
IEEE 802.4 Un estándar para capa física aprobado por el IEEE que utiliza el acceso mediante contraseña (Token passing) en una topología para red de bus.
Instituto de Ingenieros Eléctricos y Electrónicos, IEEE (Institute of Electrical and Electronic Engineers). Un organismo profesional de ingenieros que también propone y aprueba estándares.

Interconexión de Sistemas Abiertos, OSI (Open Systems Interconnection) Una familia de normas generadas por ISO relacionada con la comunicación de datos.
Interfaz. Un punto en común entre dos aplicaciones en software o dos dispositivos de hardware.
Internet. Un conjunto de redes conectadas entre sí que abarca todo el mundo y utiliza la NFSNET como columna vertebral. Internet es el término específico de una interred o de un conjunto de redes.
Interprete de protocolo, PI (Protocol Interpreter) Un proceso que lleva a cabo las funciones de FTP. FTP utiliza un intérprete de protocolo para el servidor y otro para el usuario.
Jam (Embotellamiento) Un término de Ethernet empleado para comunicarse con todos los dispositivos de una red en los que ha ocurrido una colisión.
LAN (Red de Área Local) Un conjunto de dispositivos que están conectados para permitir las comunicaciones entre sí en un solo medio físico.
Marco (Frame) Por lo general, se refiere a todo el paquete Ethernet, que incluye la información original y todos los encabezados y colas de las capas del TCP/IP (incluyendo las de Ethernet).
Mascara de dirección (También llamada Mascara para la subred). Conjunto de reglas que sirven para omitir algunas partes de una dirección IP completa, con el fin de alcanzar el destino final sin tener que utilizar un mensaje de transmisión.
Mascara de subred (Subset Mask) Un conjunto de bits que evita que las redes emitan por todo el sistema, y que en su lugar, restringe la emisión a una subred.
Modelo de referencia ISO (ISO Referente Model) El modelo para redes ISO de siete capas. Este aísla las funciones específicas que se encuentran dentro de cada capa.
Módem (Modulador-Demodulador) Un dispositivo que convierte las señales digitales en señales análogas y viceversa. Utilizado en la conversión de señales para transmisiones mediante líneas telefónicas.
Multiplexión. La transmisión simultanea de varias señales sobre un canal.
Nodo. Un término genérico utilizado para hacer referencia a los dispositivos de la red.
Paquete. En TCP/IP es un término que se refiere a la transmisión de datos entre la capa de Internet y la capa para vínculo de datos. También es un término genérico utilizado para hacer referencia a los datos transferidos a través de una red.
Peticiones de comentarios, RFC (Requests for Comments). Documentos que contienen las especificaciones para los protocolos TCP/IP. Las RFC también se utilizan para brindar nuevos protocolos. Las RFC también están disponibles desde el Centro de Información de Redes (NIC).
PING, Buscador Internet para paquetes (Paquet Internet Grouper) Un programa de utilerías utilizado para probar el software TCP/IP de un sistema al enviar una solicitud ICMP de reflejo y, luego, esperar una respuesta.
Plazo de retransmisión (Retransmisión Timeout) Ocurre cuando los datos se han enviado a un destino, pero no se ha recibido ningún acuse de recibo para el momento en que expira el tiempo. Cuando ocurre un plazo de retransmisión, el protocolo generalmente reenvía los datos.
Protocolo. Las reglas que rigen el comportamiento o el método de operación de alguno de los aspectos de una red.

Protocolo de Control de Transmisión, TCP (Transmision Control Protocol) Un protocolo para capa de transporte que es parte de la suite del protocolo TCP/IP y que proporciona un flujo de datos confiable basado en la conexión.
Protocolo Internet, IP (Internet Protocol) La parte del TCP/IP que maneja el enrutamiento.
Protocolo Internet para Mensaje de Control, ICMP (Internet Control Message Protocol). Un protocolo de mensajes de control y de error que trabaja en conjunción con el Protocolo Internet (IP).
Protocolo Inverso para Definición de Dirección, RARP (Reverse Ardes Resolution Protocol). Un protocolo TCP/IP que permite que un dispositivo adquiera su dirección IP al realizar una transmisión en la red.
Protocolo para Datagrama de Usuario, UDP (User Datagram Protocol) Un protocolo para capa de transporte que no tiene conexión. No realiza retransmisión de datos.
Protocolo para Definición de Dirección, ARP (Ardes Resolution Protocol) Un protocolo utilizado para correlacionar una dirección IP con la dirección física de la máquina. La operación inversa la realiza el Protocolo para Definición de Dirección Inversa (RARP).
Protocolo para Transferencia de Archivos, FTP. Una aplicación TCP/IP utilizada para transferir archivos de un sistema a otro.
Protocolo Punto a Punto, PPP (Point-to-Point Protocol) Un protocolo TCP/IP que proporciona conexiones del host a la red y de enrutador a enrutador. Puede utilizarse para proporcionar una conexión de línea en serie entre dos máquinas.
Protocolo Simple para Transferencia de Correspondencia, SMTP (Simple Mail Transfer Protocol) En TCP/IP, Una aplicación que proporciona servicios de correo electrónico.
Puente. Un dispositivo para red que es capaz de conectar redes que utilizan protocolos similares.
Puerto. Un numero utilizado para identificar las aplicaciones TCP/IP. Por lo general un puerto es un punto de entrada o salida.
Red. Un número de dispositivos que están conectados para permitir a cada uno de ellos comunicarse con los otros en un medio físico.
Red de Área Amplia (WAN) Termino generalmente utilizado para hacer referencia a una red que se extiende sobre grandes distancias geográficas.
Red de Área Metropolitana (MAN). Una red aprobada por el IEEE que soporta altas velocidades en un área metropolitana.
Relè de Trama (Frame Relay). Un mecanismo de comunicación de red para enlutar las tramas tan rápidamente como sea posible.
Repetidor. Un dispositivo para red que aumenta la potencia de las señales de entrada para permitir que la longitud de una red se extienda.
RIP, Protocolo de Información de Enrutamiento (Routing Information Protocol) Un protocolo TCP/IP utilizado para intercambiar información acerca del enrutamiento. Por lo común se utiliza cuando sólo está en uso un pequeño número de computadoras.
Segmento. Una unidad de datos del protocolo (PDU) que consiste en un encabezado TCP y en los datos (opcionales). También utilizado para hacer referencia a las partes de una red que esta dividida en partes mas pequeñas (segmentos).

Servidor de envío. (Push Service) Un servicio proporcionado por el TCP que permite que una aplicación especifique cuando los datos deben transmitirse tan pronto como sea posible.
Servicio de nombre de dominio, DNS (Domain Name Service) Un servicio que convierte los nombres simbólicos de los nodos en direcciones IP. DNS con frecuencia se utiliza en TCP/IP. DNS utiliza una base de datos distribuida.
Servicio de usuario. Un servicio proporcionado por el TCP que permite a una aplicación especificar que los datos que se están transmitiendo son urgentes y que deben procesarse tan pronto como sea posible.
Socket. En TCP/IP, un punto direccionable que consta de una dirección IP y un numero de puerto TCP o UDP, que proporciona aplicaciones con acceso a los protocolos TCP/IP.
Subred. En TCP/IP, parte de una red TCP/IP identificada por una parte de la dirección Internet.
SYN. Un segmento utilizado en el inicio de una conexión TCP para habilitar a ambos dispositivos, a intercambiar información que defina las características concernientes a la sesión. También se utiliza para sincronizar el dispositivo objetivo y el de destino.
Tabla de enrutamiento. (Routing Table) Una lista de las rutas de acceso válidas a través de las cuales pueden transmitirse los datos.
Tarjeta de la Interfaz de Red, NIC (Network Interface Card) Un termino genérico para un tablero (board) interfaz para redes que se utiliza para conectar un dispositivo a la red. La NIC es el lugar donde se lleva acabo la conexión física a la red.
Telnet. Una aplicación TCP/IP que permite al usuario entrar a un dispositivo remoto.
Tiempo de vida, TTL (Time-to-Live) La cantidad de tiempo que puede permanecer un datagrama en la red. Se especifica como el numero de saltos (hops) permitidos.
Token Ring. Un protocolo de capa inferior para red, basado en la conexión, que utiliza un método de acceso mediante contraseña (Token passing) para controlar el trafico de datos.
Topología. La configuración de los dispositivos de la red.
Trafico. Un término general utilizado para describir la cantidad de datos que se encuentran en la columna vertebral de una red.
Unidad de Datos de Protocolo, PDU (Protocol Data Unit) Un termino utilizado en TCP/IP para hacer referencia a una unidad de datos, encabezados y colas en cualquier capa de una red.

Bibliografía

Aprendiendo TCP/ IP en 14 días / Timothy Parker México: Prentice Hall Hispanoamericana: Sams, 1995

Using TCP-IP: workbook / by Mark Minasi Clifton, New Jersey : Data-Tech Institute, c 1994

Edición especial Redes con Microsoft TCP/IP / Drew Heywood; tr. Juan Pedro Bello; edición en español Alejandro Domínguez Doncel Madrid; México: Prentice Hall, 1999

Subnet design for efficient networks / Keith Sutherland Oxford: Butterworth-Heinemann, 2000

A.N.U.I.E.S. Anuario Estadístico 2003 Licenciatura en Universidades e Institutos Tecnológicos, 2003.

Domine TCP/IP / José Luís Raya, Víctor Rodrigo / Alfaomega.

TCP/IP for the AS/400 / Jim Hoopes, Robin Klima, Martin Pluth.

Protocolos de Internet / Angel López, Alejandro Novo / Alfaomega.

Troubleshooting TCP/IP / Mark A. Millar, P. E. /Third edition / M&M Books.

Internetworking with Netware TCP/IP / Karanjit S. Siyan, Peter Kuo, Peter Rybaczyk

TCP/IP Ilustrated Vol. 3 / W. Richard Stevens / Addison Wesley Publishing Company.

Guía práctica de Comunicaciones y Redes Locales / Antonio Cebrián Ruz / Ediciones G. Gilli S. A de C. V.

www.anuies.mx

www.hemerodigital.unam.mx/ANUIES/

www.e-mexico.gob.mx/wb2/eMex/eMex_Anuies

www.itlp.edu.mx/publica/tutoriales/guiatuto/

www.sep.gob.mx/

www.universia.net.mx/contenidos/universidades/

www.bibliojuridica.org/libros/libro.htm?l=1183