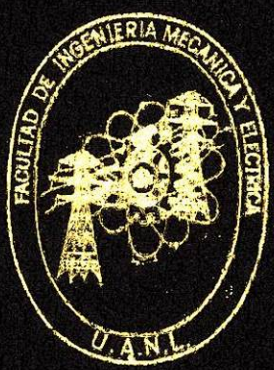
UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA



INTRODUCCION A INTERNET Y PROTOCOLO TCP/IP

CURSO

CON OPCION AL TITULO DE
INGENIERO EN ELECTRONICA Y COMUNICACIONES

PRESENTA

ADRIAN DE JESUS HERNANDEZ DELFIN

ASESOR: ING. JOSE RIVERA MARTINEZ

CD. UNIVERSITARIA

DICIEMBRE DE 1995

UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE INGENIERIA MECANICA
Y ELECTRICA

INTRODUCCION A INTERNET Y PROTOCOLO TCP/IP.

CURSO

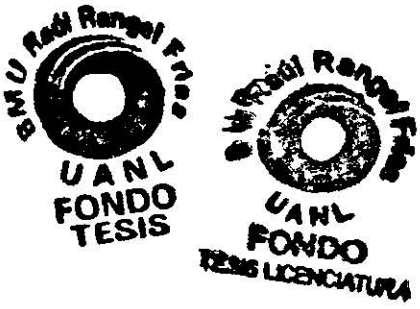
CON OPCION AL TITULO DE
INGENIERO EN ELECTRONICA Y COMUNICACIONES

PRESENTA

ADRIAN DE JESUS HERNANDEZ DELFIN

ASESOR: ING. JOSE RIVERA MARTINEZ

CD. UNIVERSITARIA DICIEMBRE DE 1995



Universidad Autónoma de Nuevo Loen

Facultad de Ingeniería Mecánica y Eléctrica

Curso con opción a título:

Conectividad

Asesor :Ing. José Rivera Martínez

Tesina :

Introducción a Internet y Protocolo TCP/IP

Adrián de Jesús Hernández Delfín

Ingeniero en Electrónica y Comunicaciones

Matricula : 731644

DEDICATORIA :

Dedico este trabajo a todas las personas que sin necesidad de estar aquí me dieron su apoyo incondicional y también a los que estuvieron aquí pues siempre es necesario alguien cerca de uno. Gracias amigos !!

También quiero dedicarlo a mis hermanos y demás familiares, unos por soportarme y los otros por confiar en mi y por su apoyo.

Pero quiero dedicarlo especialmente a mis padres Elvina Delfín de Hernández y José Lara Hernández por permitir - con todos sus esfuerzos y sacrificios- terminar este sueño que les devuelvo hecho realidad

Mil Gracias !!!

Agradecimientos :

Agradezco a todos los maestros, catedráticos, profesionistas, familiares y amigos que de una u otra forma me enseñaron lo poco que ahora se y me llevaron a lo que soy y me apoyaron durante todos estos años de estudio.

Contenido :

¿Que es Internet ?

Internet nació hace cerca de 20 años, surgió por el esfuerzo de interconectar la red ARPAnet del departamento de defensa estadounidense con varias redes enlazadas por medio del satélite y de radio. ARPAnet era una red experimental que apoyaba la investigación militar, en particular la investigación sobre como construir redes que pudieran soportar fallas parciales (como las producidas por bombarderos) y aun así funcionar. En el modelo Arpanet, la comunicación siempre ocurre entre una computadora fuente y una destino. La red asume que es falible, fue diseñada para requerir información de las computadoras que forman parte de ella. Para enviar un mensaje en la red, una computadora solo tiene que poner la información en un sobre, llamado paquete de protocolo Internet (IP: Internet Protocol) y le asigna el domicilio destino en la forma correcta. Las computadoras que se comunican -no la red- tienen la responsabilidad de asegurar que la comunicación se lleve a cabo. La filosofía principal era que cada computadora en la red se pudiera comunicar, como un elemento individual, con cualquier otra computadora.

Los desarrolladores de Internet en Estados Unidos, el Reino Unido y Escandinavia, en respuesta a las presiones del mercado, empezaron a poner software de IP en todo tipo de computadoras. Se llego a convertir en el único método practico para comunicar computadoras de diferentes fabricantes. Esto resulto muy atractivo para el gobierno y las universidades, quienes no tenían políticas que especificaban la compra de una determinada marca de computadoras.

Al mismo tiempo que Internet se consolidaba, las redes locales Ethernet eran desarrolladas. La tecnología de las redes locales maduro hasta 1983, cuando aparecieron las primeras estaciones de trabajo para escritorio y las redes locales se multiplicaron. La mayor parte de las estaciones de trabajo tenían el sistema UNIX de Berkeley instalado, que incluía el software de red IP. Esto creo una nueva demanda : en lugar de conectar una computadora de tiempo compartido en un centro de computo, las organizaciones requerían conectar toda su red local a ARPAnet, lo cual permitía que todas las computadoras de la red usaran los servicios de ARPAnet. Al mismo tiempo muchas compañías y otras organizaciones empezaron a construir redes privadas usando los mismos protocolos de comunicación de ARPAnet, es decir IP y sus protocolos asociados. Parecía obvio que si estas redes se podían comunicar

entre si, los usuarios de una red podrían comunicarse con usuarios de otra y todo el mundo seria beneficiado.

De estas nuevas redes, una de las más importantes fue la NFSNET, auspiciada por la Fundación Nacional de la Ciencia (NFS : National Science Foundation), una agencia de gobierno de E.U., al final de los ochenta la NSF creo cinco centros de supercomputo en universidades importantes. Hasta ese entonces, las computadoras más rápidas del mundo solo estaban a disposición de los fabricantes de armamento y de algunos investigadores de compañías muy grandes. Con la creación de centros de supercomputo, la NSF ponía estas fuentes a disposición de cualquier investigación escolar, solo se crearon cinco centros por que su costo era elevado y fue necesario compartirlos. Esto provoco un problema de comunicación : se necesitaba interconectar a los centros y permitir a los usuarios tener acceso a ellos. Al principio, la NSF trato de utilizar la red ARPAnet para la comunicación de los centros, pero esta estrategia fallo debido a problemas burocráticos

En respuesta a esto, la NSF decidió construir su propia red basada en la tecnología IP de ARPAnet. Esta red conectada a los centros mediante enlaces telefónicos de 56000 bits por segundo. Sin embargo, era obvio que si se trataba de conectar cada universidad a los centros de supercomputo, el proyecto se podría venir abajo. El costo de la línea telefónica depende de la distancia. Una línea por universidad con un centro de supercomputo como eje, requeriría de muchas metros de líneas telefónicas, por esta razón se decidió crear redes regionales. En cada región del país las escuelas podían conectarse a su vecino más cercano, cada cadena estaba conectada a un centro de supercomputo en un solo punto. Con esta configuración, cualquier computadora podría eventualmente comunicarse con otra, fomentando la comunicación entre los vecinos.

Esta solución fue un éxito y, como cualquier solución exitosa, llego el momento en que dejo de funcionar. El hecho de compartir supercomputadoras permitió a los centros de computo compartir recursos no relacionados con los centros; repentinamente, las escuelas que participaban en la red contaron con un amplio universo de información y colaboradores al alcance de su mano. El trafico en la red se incremento con el tiempo hasta que las computadoras que las controlaban y las líneas de teléfono conectadas a ellas se saturaron. En 1987 se celebro un contrato para administrar y actualizar la red, con la compañía Merit Network Inc., que operaba la red educacional de Michigan,

en colaboración con IBM y MCI. La vieja red fue mejorada con líneas telefónicas de mayor velocidad y con computadoras más poderosas.

El aspecto más importante del esfuerzo de conectividad de la NSF fue, el hecho de permitir a todos el acceso a la red. Hasta entonces, el acceso a Internet solo estaba permitido a investigadores de ciencias computacionales, empleados y contratistas del gobierno. La NSF promovió el acceso universal a las instituciones educativas, financiando conexiones en las universidades únicamente si estas tenían un plan para permitir el acceso a la zona. De esta manera, toda persona que estuviera inscrita podría ser usuario de Internet.

La demanda sigue creciendo, ahora que la mayoría de las universidades esta conectada, se esta tratando de incluir también a primarias y secundarias, al igual que las bibliotecas locales. Las personas que recientemente se graduaron en un universidad saben para que sirve Internet y hablan con sus compañeros de trabajo acerca de conectar la empresa en que laboran a dicha red. Toda esta actividad apunta a un crecimiento continuo, a la solución de problemas de conectividad, la evolución de las tecnologías y a la seguridad en el empleo de los expertos en comunicaciones. Mucha gente va más allá; pues una vez que se cuenta con una conexión de red en el trabajo, el siguiente paso lógico es conectarse directamente desde su casa.

¿ Que compone a Internet ?

Como esta compuesta Internet es una pregunta difícil de contestar, la respuesta cambia con el paso del tiempo pues hace cinco años hubiera sido sencillo contestar que se compone de todas las redes que utilizan el protocolo IP y cooperan para formar una sola red para dar servicios a los usuarios colectivos. Esto incluiría a varias redes federales, un conjunto de redes regionales, redes de centros universitarios y algunas redes de otras partes del mundo.

Más recientemente, algunas redes que no utilizaban el protocolo IP se dieron cuenta de que Internet era una buena opción. Y quisieron proveer a sus clientes de acceso a la red, así que se desarrollaron métodos para conectar estas extrañas redes (por ejemplo, BITNET, redes DECnets, etc.) a Internet. Al principio estas conexiones llamadas *puertas*, servían únicamente para transferir correo electrónico entre las dos redes. Algunas, sin embargo, han llegado a utilizarse para transferir servicios entre las redes.

La máxima autoridad sobre la cual descansa Internet es la Sociedad Internet (ISOC: Internet Society). La ISOC es una organización de membresía voluntaria cuyo propósito es promover el intercambio de información a nivel global mediante el uso de la tecnología de Internet. Esta designa a una especie de consejo cuya responsabilidad consiste en la administración técnica y la dirección de Internet. Quienes integran la ISOC son un grupo de voluntarios invitados llamado Consejo de Arquitectura de Internet (IAB: Internet Architecture Board). El IAB se reúne con regularidad par dar standares y asignar recursos, como los domicilios. Internet funciona porque existen formas estándar para que las computadoras y las aplicaciones de software se comuniquen entre si. Esto permite que las computadoras de diferentes fabricantes puedan comunicarse sin ningún problema. Internet no es una red de equipos IBM, SUN o Macintosh. El IAB es el responsable de estos estándares : decide cuando es necesario un estándar y como debe ser. Cuando se requiere un estándar, se considera el problema, se adopta el estándar y se anuncia a través de la red. El IAB lleva también un registro de algunos números (y otras cosas) que deben ser únicos. Por ejemplo, cada computadora en Internet debe tener un domicilio único de 32 bits y ninguna otra puede tener el mismo domicilio. ¿ Como se asigna el domicilio ? El IAB se encarga de resolver este tipo de asuntos. En realidad no es quien asigna el domicilio, pero establece las reglas para la asignación.

Nadie paga por el servicio; no existe la empresa Internet Inc. que cobre cuotas a las redes de Internet o a los usuarios. En lugar de ello, todos pagan su parte, la NSF paga por la NFSNET; la NASA paga por la NASA Science Internet; la U.A.N.L. paga por la RED UANL. Las redes se reúnen para decidir como conectarse y como pagar la interconexión. Una escuela u organización paga por su conexión a una red regional, la cual a su vez paga por el acceso a un proveedor de servicios a nivel nacional.

Existe el mito de que Internet es gratis, no lo es, alguien paga por cada conexión de Internet. Muchas de estas cuotas no llegan hasta el usuario final, lo que da la ilusión de acceso gratuito. Pero existen muchos usuarios que saben que Internet no es gratis, pues pagan mensualmente o por hora los cargos por el acceso desde su casa, a velocidades superiores a los 56 Kb por segundo.

Los usuarios generalmente se acuerdan de quien les transmite sus llamadas cuando ocurre algún problema. Si un conmutador se descompone, solo la compañía telefónica puede componerlo, las compañías telefónicas pueden hablar entre si para resolver un problema pero cada una deberá resolver los propios. Lo mismo se aplica a Internet, cada red tiene su centro de operaciones de la red (NOC: Network Operation Center). Los centros de operaciones se comunican entre si y saben como resolver sus problemas.

Nuevos estándares de protocolos

Cuando se menciono como se inicio Internet, se hablo de la Organización Internacional para la Estandarización y su conjunto de protocolos. Finalmente se termino de diseñar. Ahora es un estándar internacional, al que se conoce comúnmente como conjunto de protocolos ISO/OSI (Interconexión de Sistemas Abiertos : Open Systems Interconnect). Hoy en día muchos de los componentes de Internet permiten el uso de los protocolos OSI. Todavía no existe mucha demanda. El gobierno estadounidense a tomado una postura en la que define que todas sus computadoras deben ser capaces de manejar estos protocolos. Muchas cuentan con el software, pero muy pocas lo utilizan.

Internet ha sido por mucho tiempo una red internacional, pero solo se había extendido hacia los países que mantenían buenas relaciones diplomáticas con Estados Unidos y hacia las bases militares de este país que están fuera de su territorio. Ahora, con una situación menos tensa internacionalmente hablando, Internet se ha esparcido por todos lados. Actualmente se encuentra en más de 60 países y el numero esta creciendo rápidamente. Los países de Europa Oriental han querido participar desde mucho tiempo atrás, pero fueron excluidos por las regulaciones del gobierno. Ahora con la cortina de acero destruida, estos países figuran en Internet. Los países del tercer mundo (como México) que anteriormente no contaban con los recursos para participar en Internet, la ven ahora como un medio para elevar sus niveles educativos y tecnológicos.

En Europa, el desarrollo de Internet solía ser obstruido por políticas nacionales que ordenaban el uso de los protocolos OSI y consideraban al IP como un intruso cultural similar a EuroDisney. Fuera de Escandinavia (donde adoptaron los protocolos IP desde hacia mucho tiempo), estas políticas evitaron el desarrollo de grandes redes Internet. En 1989, RIPE (Reseaux IP Europeens) comenzó a coordinar la operación de Internet en Europa; hoy en día, el 25% de los equipos anfitriones conectados a Internet se encuentran en este continente.

En estos momentos, la expansión internacional de Internet se ha visto impedida por la falta de infraestructura de comunicaciones; o mejor dicho, de un buen sistema telefónico.

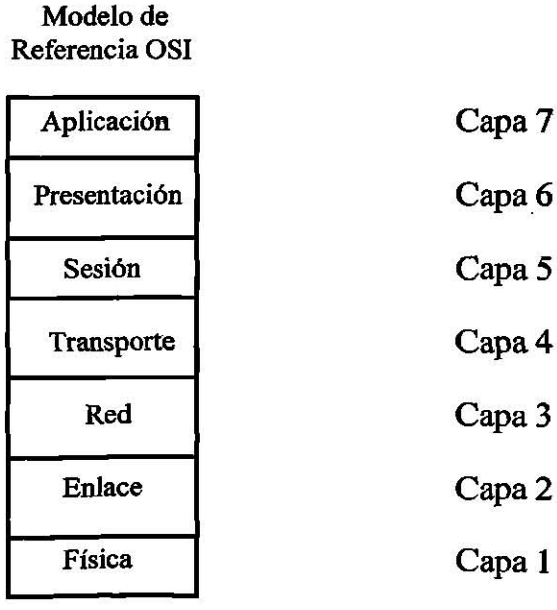
Como trabaja Internet

Es bueno saber un poco sobre como funcionan las cosas, pues permite entender algunos de los consejos que se mencionan en esta tesis, para que no parezcan reglas arbitrarias que se deben aprender por rutina. Esto se analizara con el mayor detalle posible para facilitar su comprensión, pero no se vera nada de diseño de redes.

Aquí se verán las redes de conmutación de paquetes y como, poniendo el protocolo TCP/IP a trabajar en este tipo de redes, se puede hacer algo útil.

Se hablara acerca del protocolo básico que predomina en las comunicaciones de internet : el TCP/IP. Este es el bloque sobre los que esta cimentada Internet, (también se basa en el protocolo UDP). También se vera un poco sobre el Sistema de Nomenclatura de Dominios y algunas aplicaciones.

El sistema de redes moderno esta construido sobre el concepto de *niveles o capas de servicio.* El intercambio de información se basa en el movimiento de bits de un lado a otro teniendo en ocasiones perdidas de estos bits en el trayecto. Este nivel se compone de cables y hardware, y no necesariamente de cables muy confiables. Después, se agrega una capa de software básico que permite aislar los problemas del hardware. Incorpora otra capa de software para dar al software básico algunas características deseadas. Continua agregando funcionalidad e inteligencia a la red, capa por capa, hasta que obtiene algo amigable y útil.

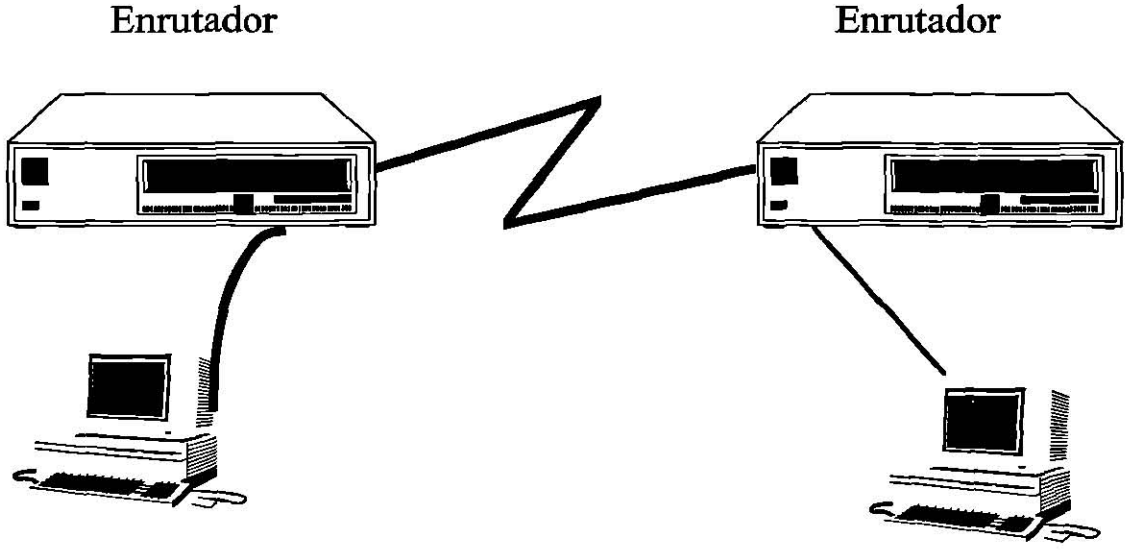


Redes de conmutación de paquetes

Cuando se trata de imaginar que es Internet y como opera, se piensa en un sistema telefónico, pues Internet esta compuesta principalmente por líneas telefónicas permanentemente dedicadas a este uso. La red telefónica es una red de conmutación de circuitos, cuando uno habla se separa la línea utilizada de las demás para atender la llamada esto hace inaccesible a otras personas a esta línea, lo que provoca estar utilizando un recurso muy costoso: la red.
Para entender lo de ***conmutación de paquetes,*** Internet lo que hace con los mensajes a transmitir es mezclarlos todos, se pone en el medio de transmisión, se transfiere hacia el lugar y se clasifica.

El Protocolo Internet, IP

Ya se sabe que Internet puede hacer que la información viaje y llegue a distintos lugares distribuidos por todo el mundo. Las diferentes partes de Internet están conectadas por un conjunto de computadoras llamadas ***enrutadores,*** que interconecten a las redes. Estas pueden ser Ethernet, token rings o en ocasiones líneas telefónicas, como se muestra en la figura 1.



Las líneas telefónicas y las redes Ethernets son el medio a través del cual el correo va de un lugar a otro. Los ***enrutadores*** deciden como dirigir la información (paquetes), no todos los enrutadores cuentan con una conexión a cada uno de los otros enrutadores de la red, esto significa que cada enrutador solo necesita conocer las conexiones con las que cuenta y cual es el camino más rápido para acercar el paquete a su destino ósea que escoge el enlace más apropiado para enviar la información.

El protocolo Internet IP se hace cargo de establecer domicilios o se asegura de que los enrutadores sepan que hacer con la información que les llega. Una parte de la información del domicilio va al principio del mensaje, los domicilios de Internet constan de 4 números, cada uno menor que 256, dichos números se separan por puntos, como se muestra a continuación :

192.112.36.5

128.174.5.6

Los primeros números indican a los enrutadores la red a que pertenece dicho domicilio, los últimos indican que computadora personal o equipo debe recibir el paquete, cada computadora en Internet tiene un domicilio único.

por muchas razones practicas la información enviada a través de las redes IP se divide en pedazos de tamaño distinto, llamados ***paquetes***. La cantidad de información en un paquete normalmente se encuentra entre 1 y aproximadamente 1500 caracteres de largo.

El protocolo de Control de Transmisión (TCP)

El TCP es el protocolo que se menciona junto con el IP y que se utiliza para resolver todo tipo de problemas en los enlaces entre redes, este protocolo toma la información que se desea enviar y la divide en segmentos, además enumera cada segmento para que el receptor pueda verificar la información y ponerla en el orden adecuado. Para que el protocolo TCP pueda enviar esta secuencia de números (domicilios) a través de la red, cuenta con su propio sobre que le permite escribir en el la información requerida para su ordenamiento. Un segmento de la información a transmitir se coloca en el sobre del protocolo TCP, este sobre es puesto, a su vez, dentro del sobre del protocolo IP y posteriormente es transmitido a la red.

Del lado del receptor, el software de TCP reúne los sobres y extrae la información de ellos y la pone en el orden adecuado. Si algún sobre se pierde en la transmisión, el receptor solicita su retransmisión al emisor, una vez que

el protocolo TCP tiene toda la información en el orden adecuado, la pasa a la aplicación del programa que este utilizando.
El TCP resuelve este tipo de problemas como cuando se pierde un paquete de información o son modificados por el mal funcionamiento durante la transmisión a través de las líneas telefónicas.
Este protocolo calcula lo que llamamos ***numero de verificación (checksum),*** este numero permite al receptor TCP que detecte errores en el paquete transmitido, cuando un paquete llega a su destino, el receptor calcula el numero de verificación y lo compara con el enviado por el transmisor; si no coinciden significa que ocurrió un error en la transmisión y el receptor deshecha el paquete y solicita la retransmisión.
El protocolo TCP crea la apariencia de que existe una conexión permanente entre dos aplicaciones, garantizando de esta forma que lo que se transmite de un lado llegue al otro. Realmente no se cuenta con un enlace directo entre el emisor y el receptor pues otras personas pueden usar los mismos enrutadores y la red de cableado en los lapsos que ocurren entre el envío de cada paquete, pero, para propósitos prácticos pareciera que si.

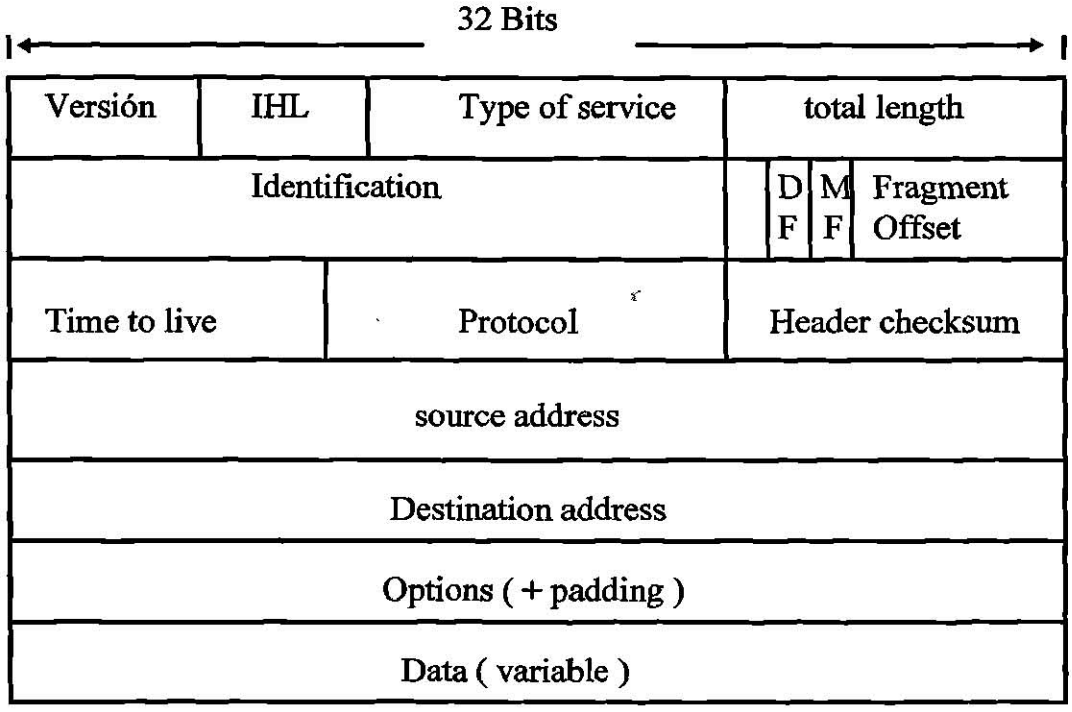
TCP/IP : Introducción

TCP/IP es una forma abreviada de referirse al protocolo estándar del Departamento de la Defensa (DOD) de los Estados Unidos llamado "TRANSMISSION CONTROL PROTOCOL/ INTERNET PROTOCOL". Estos protocolos implementan los niveles de transporte y soporte de red, respectivamente, del modelo OSI, y son la parte central de diferentes redes usadas en instituciones militares, así como en muchos institutos de investigación, universidades y fabricantes de equipo computacional.
Mientras que TCP/IP puede en teoría ser usado en cualquier hardware apropiado de interconexión, en la practica, TCP/IP es soportado sobre distintas configuraciones estándar de hardware.
Las redes locales basadas en Ethernet, son la configuración de hardware preferida para la versión de TCP/IP que corre en el Berkeley UNIX. Esta usa la especificación de Ethernet de 10MBPS en cable coaxial. Puede soportar hasta varios cientos de equipos centrales en una red dada dentro de una distancia de un kilometro (más con repetidores). Estas redes permiten a los sistemas acceso a los archivos, a través de la red.

Ethernet proporciona un camino entre todos los procesadores que están en la red, de manera que cualquier procesador pueda comunicarse con cualquier otro de la red, pero solo una transferencia (paquete) puede estar activa en la red a un tiempo dado. el acceso a la red es controlado vía CSMA/CD (Carrier Sense Multiple Access/Collision Detect). Cada computadora en la red, monitorea todo el trafico, y detiene un mensaje cuando detecta que es dirigido hacia ella.
Esencialmente todas las conexiones de hardware de TCP/IP soportan la idea de "GATEWAYS" entre diferentes redes, debido a esto, un usuario no necesita familiarizarse con el medio actual utilizado en alguna parte de la red. en la practica cualquier usuario que tenga acceso a una red Ethernet, puede implementar una solución basada en TCP/IP utilizando componentes estándar para las computadoras más populares de hoy en día.

Capa de Red

IP es protocolo primario de la capa 3 de Internet. Además de proporcionar ruteos en redes interconectadas, IP también proporciona una forma de fragmentar y reensamblar los datagramas y puede manejar reportes de errores. Junto con TCP, IP representa el corazón del protocolo de Internet. El formato del paquete de datos de IP se muestra en la siguiente figura.

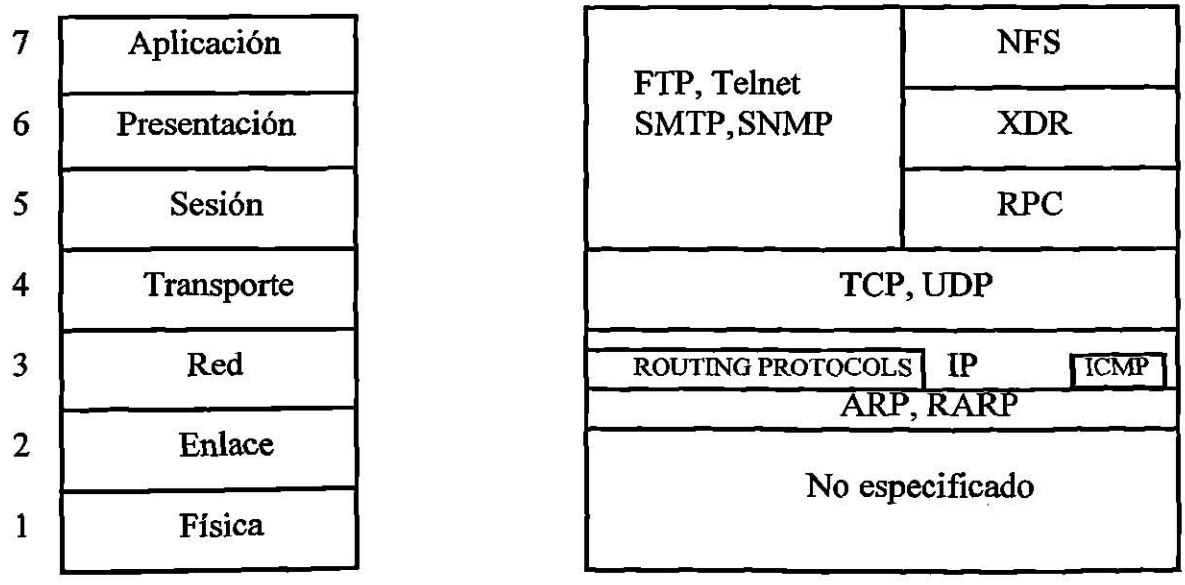


* El encabezado de IP empieza con un numero de versión, el cual indica la versión de IP que actualmente se esta utilizando.
* El campo de *IP Header lenght* (IHL) indica el encabezado del datagrama de una longitud en palabras de 32 bits
* El campo de *Type of service* especifica como debe ser controlado un particular protocolo de las capas superiores semejante al actual datagrama, a estos datagramas se le pueden asignar varios niveles de importancia a través de este campo
* El campo de *Total lenght* especifica la longitud total del paquete de IP, incluyendo datos y encabezados en bytes
* El campo *Identification* contiene un numero que identifica el datagrama actual. Este campo es usado para ayudar a juntar las partes de un datagrama fragmentado

Protocolos Asociados

El conjunto de protocolos de TCP/IP corresponden en cierta medida al Modelo de Red de Comunicaciones de la Organización Internacional de Estándares (ISO). Este modelo es llamado Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI). El modelo OSI describe un Sistema de Red de Computadoras Ideal en el cual las comunicaciones sobre la red ocurren entre procesos a niveles discretos e identificables. Cada nivel en un equipo dado, proporciona servicios a los niveles superiores y a su vez, recibe servicios de los niveles inferiores a el. El sistema de niveles permite a los desarrolladores concentrar sus esfuerzos en las funciones a un nivel dado. No es necesario para ellos crear todos los mecanismos para enviar información a través de la red. Ellos necesitan conocer solamente que servicios necesita proporcionar el software a los niveles superiores, y que servicios pueden proporcionarle los niveles inferiores, y cuales protocolos del conjunto de protocolos proporcionan esos servicios.

Modelo de referencia OSI y Protocolo TCP/IP



* El campo *Flags* (conteniendo un bit DF, un bit MF y un fragmentado de Offset), especifica si el datagrama puede ser fragmentado y si el actual fragmento es el final
* El campo *Time to live* permite a un contador que gradualmente se decrementa hasta cero, en donde el datagrama es descartado. Estos paquetes se guardan como lazos interminables
* El campo *Protocol* indica cual protocolo de las capas superiores recibe nuevos paquetes una vez que el proceso de IP este completo
* El campo *Header checksum* ayuda asegurando la integridad de los encabezados de IP.
* Los campos *Source y destination address* especifican los nodos que enviaran y recibirán información
* El campo *Options* permite a IP soportar varias opciones, tal como seguridad
* El campo *Data* contiene información para las capas superiores

Direcciones Físicas y Direcciones Internet

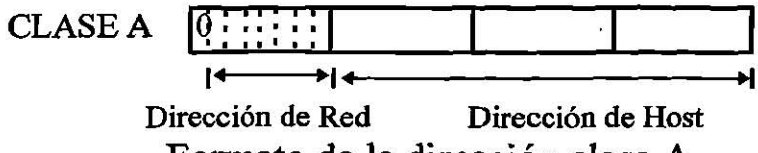
En el nivel de enlace, los nodos en una red se comunican con otros nodos en base a una dirección especifica. Un nodo en una Red puede ser una microcomputadora, un servidor de archivos, una impresora, o cualquier otro dispositivo con su propia implementación de TCP/IP. Cada nodo tiene una Dirección Física especifica al Hardware que los conecta a la Red. La dirección física tiene diferentes formas en redes diferentes y ellas son asignadas de diferentes maneras. Por ejemplo, una dirección física en una red Ethernet es un valor numérico de 6 Bytes, como 08-15-20-37-89-79, este es asignado por el fabricante de la tarjeta de red. Las redes basadas en el estándar X.25 de CCITT usan el estándar X.21 para direcciones físicas, el cual consiste de un numero de 14 dígitos. Las Redes LocalTalk usan una dirección de 3 bytes, consistente de 2 bytes para el numero de red y un byte para el numero de nodo.
Por otro lado, las direcciones Internet (IP address) son direcciones lógicas, esto es, independientes de cualquier configuración particular de hardware y tiene la misma forma sin importar el tipo de Red. Esta dirección es un numero de 4 Bytes (32 Bits) que identifica a una red y un nodo. La dirección IP de 4 bytes es representada usualmente en notación decimal separada por puntos (por ejemplo 151.31.2.12).
Los nodos trasladan la dirección IP del destino en una dirección física cuando van a enviar paquetes a otros nodos de la red. Cada aplicación que

envía información, envía también en el paquete su propia dirección IP. La aplicación que recibe el paquete, puede responder a la aplicación que se lo envío usando la dirección de este que esta incluida en el paquete.
Debido que las direcciones IP no dependen de un tipo en particular de red, ellas pueden ser usadas para enviar paquetes de información de un tipo de red a una red de otro tipo. En cada tipo de red, el software de TCP/IP efectúa la correspondencia entre direcciones físicas de direcciones IP en su red. Si un paquete información es transmitido hacia otra red, el software de TCP/IP convierte la dirección IP del destino a una dirección física apropiada para esta red. La aplicación receptora usa la dirección IP del transmisor, la cual fue incluida en el paquete de información, para responderle en la misma manera.

Direccionamiento de Internet (IP)

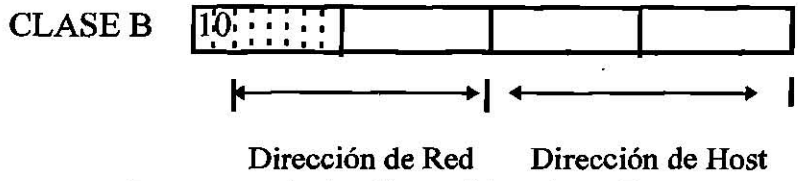
Como todos los protocolos de las capas de red, el esquema de direccionamiento de IP es integral para proceso de ruteo de datagramas de IP a través de una interred de trabajo. Una dirección de IP consta de 32 bits de longitud, dividido en dos o tres partes. La primera parte señala la dirección de la red, la segunda (si esta presente) indica la dirección de subred y la parte final indica la dirección del Host. La dirección de subred están presentes solo si el administrador de la red tiene decidido que la red debería ser dividida en varias subredes, mas adelante mencionare algo al respecto de estas subredes. Los tamaños de las longitudes de la red, la subred y la extensión del host son todos variables.
La dirección de IP soportan cuatro diferentes clases de red, la parte más significativa de los bits indican la clase de red.

Las redes **clase A** son proyectadas principalmente para usarse en redes muy grandes o sea de una gran cantidad de nodos, ya que proporcionan solo 7 bits para el campo de direccionamiento de red y un campo de dirección local de 24 bits, el bit de orden superior es establecido como 0, como se muestra en la figura.



Formato de la dirección clase A

Las redes **clase B** asignan 14 bits para el campo de dirección de red y 16 bits para el campo de dirección de un host. Esta clase de dirección propone una buena relación de espacio entre las dirección de red y la de host. Esta clase indica que los bits de orden superior están establecidos como 10 y su formato esta indicado en la siguiente figura.



Formato de la dirección clase B

Las redes **clase C** asignan 21 bits para el campo de dirección de la red. Las redes clase C solo proveen 8 bits para el campo de host, sin embargo el numero de host por red puede ser un factor limitante (255 host´s por red), los bits del orden superior están establecidos como 110 y el formato de esta clase esta representado en la siguiente figura.

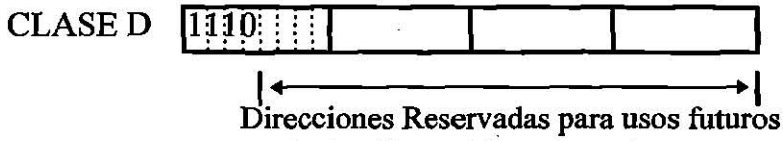
Formato de la dirección clase C

Dentro de las direcciones de **clase D** existen dos tipos :

- Las que son reservadas ya sea para grupos multiaspecto como son descritos formalmente en el RFC 1112, en el cual, se establece que los cuatro bits de orden superior son establecidos como 1110

- Las que son reservadas para usos futuros. En la este tipo de dirección de clase D los cuatro bits de orden superior son establecidos como 1.

De cualquier manera, las direcciones de clase D no están bien definidas para un uso en especial, es por eso que reciben el nombre de *Direcciones Reservadas,* ya que hasta el momento no hay software que soporte dichas direcciones o no esta al alcance de instituciones. El formato de esta clase se muestra en la siguiente figura.



Formato de la dirección clase D.

Para entender mejor el uso de estas direcciones de IP diremos que estas están divididas en cuatro secciones que llamaremos octetos (cada uno consta de 8 bits) y que en notación binaria cada uno de estos octetos puede tomar una dirección desde el 0 (00000000) hasta el 255 (11111111). El valor de cada octeto es especificado como un numero decimal y los octetos son separados por puntos por ejemplo : 192.112.35.5 o 128.174.5.6.

Para darnos una idea del alcance en cuanto al numero de nodos que pueden interactuar y ser parte de la gran red de Internet, se analizara matemáticamente que si cada octeto, puede tomar hasta un numero del 1 al 255 - el cero no se toma en cuenta - el numero de nodos que podrían existir dentro de Internet seria de 4,228,250,625 nodos, esto nos haría suponer que esta cantidad seria imposible de alcanzar y más aun de administrar, pero no es así; al estar las direcciones de IP clasificadas como clases de redes, el numero de nodos disminuiría notablemente. Es por esto que las redes tendrían un numero limitado de nodos que pudieran ellos conectar y a su vez administrar.

Analizaremos ahora en forma de síntesis cada clase de red.

- Red clase A

Direcciones posibles	0 - 127 (nnn.///.///.///)
Redes que pueden existir	128 redes
Numero de nodos por cada red	255x255x255=16,581,375 nodos

La dirección de red esta especificada por el primer octeto y el de la dirección de host por los siguientes tres octetos.
NOTA : la dirección 0.0.0.0 no existe o no esta definida para una red especifica.

- Red clase B

Direcciones posibles	128 - 191 (nnn.nnn.///.///)
Redes que pueden existir	64 x 255 = 16320 redes
Numero de nodos por cada red	255x255=65,025 nodos

La dirección de red esta especificada por los primeros dos octetos y el de la dirección de host por los restantes dos octetos.

- Red clase C

Direcciones posibles	192 - 223 (nnn.nnn.nnn.///)
Redes que pueden existir	32 x 255 x 255 = 2080800 redes
Numero de nodos por cada red	255 nodos

La dirección de red esta especificada por los primeros tres octetos y el de la dirección de host por el octeto restante.

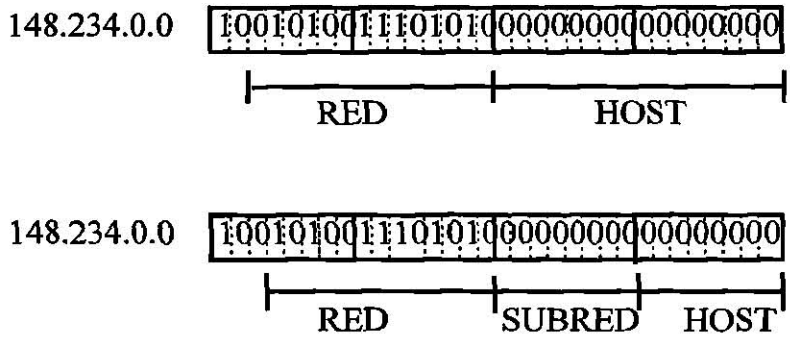
- Red clase D

Direcciones posibles	224 - 255 (Reservadas)
Redes que pueden existir	No esta definido
Numero de nodos por cada red	No esta definido

Esta clase de red, no tiene definido las redes posibles que puede haber ni el numero de nodos que cada una de ellas puede administrar, es por eso que llevan el titulo de direcciones reservadas para usos futuros.
En lo anterior "nnn" representa parte o toda la dirección de red y "///" representa parte o toda la dirección local.

Subnet Mask

Las redes IP también pueden ser divididas en unidades más pequeñas llamadas subredes. Las subredes proveen extraflexibilidad para el administrador de la red, si tomamos en cuenta que tenemos a nuestra disposición una gran cantidad de nodos (generalmente aplicados en redes clase A y B). Por ejemplo supongamos que una red tiene asignado una dirección clase B y que todos los nodos de la red actualmente están constituidos como una dirección clase B (65,025 nodos). Entonces supongamos que la representación en punto decimal de esta dirección de red es 148.234.0.0 (hay que imaginarse que todos los ceros en el campo de host, especifican una dirección total de la red). Algo que cambie todas las direcciones como algún otro numero básico, haría que el administrador pueda subdividir la red conviertiendola en subredes, esto se realiza a través del préstamo de bits de la porción de dirección de host y usar estos como un campo de subred, como esta descrito en la siguiente figura.

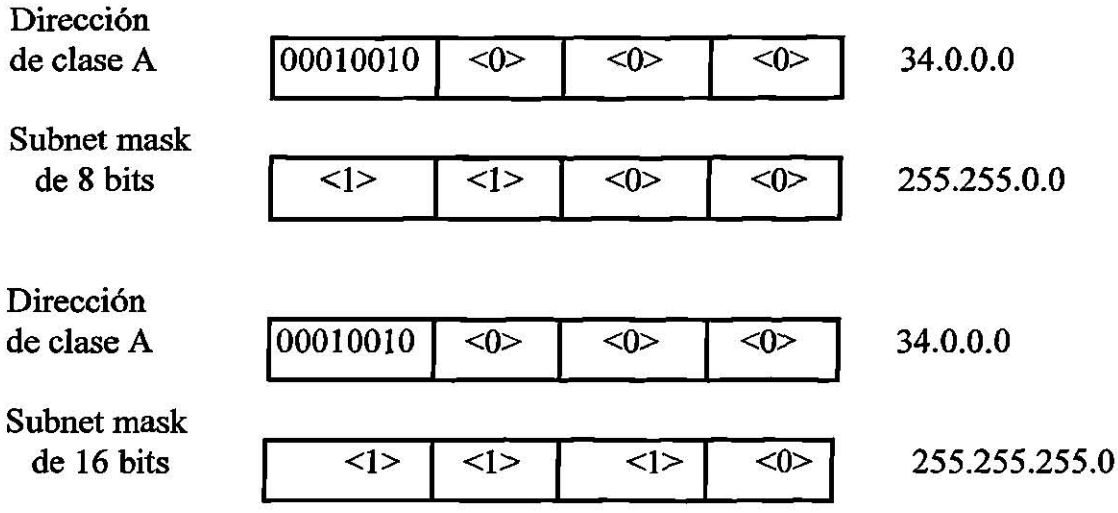


Formato de los campos de la dirección 148.234.0.0, antes y después de tener un nuevo campo que es el de la subred.

Si el administrador de la red escoge 8 bits para el campo de subred, la tercera parte de la dirección IP clase B provee el numero de subred. En el ejemplo, la dirección 148.234.1.0 indicara que la dirección de red es 148.234 y el de la subred es 1, la dirección 148.234.2.0 indica la red 148.234, subred 2 y así sucesivamente.

El numero de bits de préstamo para la dirección de subred es variable, para especificar que tantos bits son usados, el IP proporciona el ***Subnet Mask***. El subnet mask usa el mismo formato y representación técnica que una dirección de IP, el subnet mask tiene 1´s en todos los bits (255), a excepción de esos bits que especificaran el campo del host.

Por ejemplo, para una dirección de clase A 34.0.0.0, el subnet mask que especifica 8 bits para el campo de subred, seria el siguiente formato 255.255.0.0 para la misma dirección, si especificamos que queremos 16 bits en el campo de subred, el formato de subnet mask es 255.255.255.0, ambos subnets mask son mostrados en la siguiente figura



Generalmente, los campos de subred están especificados en campos de 8 y 16 bits, pero esto no quiere decir que son los únicos; hay ciertos factores que podrían alterar este numero de bits. Solo el administrador de la red seria el único capacitado a especificar la longitud del campo de subred.

La siguiente tabla indica los tipos de subnet mask que generalmente se aplican a las diversas clases de red.

Clase	subred mask	No. de redes	No. de subredes	No. de nodos
A	255.0.0.0	1	- - - -	16,581,375
	255.255.0.0	1	255	65,025
	255.255.255.0	1	65,025	255
B	255.255.0.0	1	- - - -	65,025
	255.255.255.0	1	255	255
C	255.255.255.0	1	- - - -	255

ARP y RARP

En algunos medios como el IEEE 802 LANS, el medio de dirección y las direcciones de IP son dinámicamente descubiertas a través del uso de dos o más miembros del protocolo de internet : el ***Address Resolution Protocol (ARP)*** y el ***Reverse Address Resolution Protocol (RARP).*** El ARP usa el envío de mensajes para determinar la dirección de hardware (MAC-layer) correspondiente a una dirección particular de interred de trabajo. El ARP es suficientemente genérico para permitir el uso de IP virtualmente con cualquier tipo de mecanismo haciendo transparente el acceso al medio. RARP usa el envío de mensajes para determinar la dirección de internet asociado con una dirección particular de hardware. El RARP es particularmente importante para nodos sin disco, por donde no conozcamos su dirección de internet, cuando se inicializa.

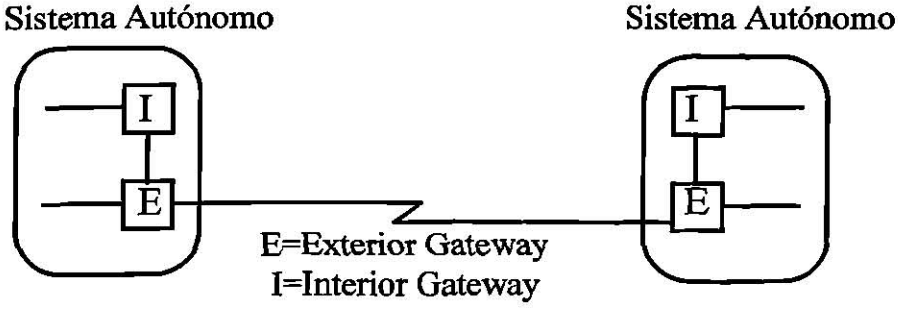
Ruteo en Internet

Los dispositivos de ruteo en Internet son tradicionalmente llamados ***Gateways*** un termino mal empleado ya que, en otro lado de la industria, el termino se aplica a dispositivos con funcionalidad algo diferente (generalmente a dispositivos que interconectan redes de diferente topologías), los gateways dentro de Internet son organizados jerárquicamente.
Algunos routers son usados para mover información a través de un grupo particular de redes bajo el mismo control y autoridad administrativa, llamada sistema autónomo; es decir, que tanto el nodo fuente como el nodo destino están en la misma red lógica, dentro de una Internet. Los routers usados para intercambiar información dentro de los sistemas autónomos son llamados ***interior routers*** y ellos usan una variedad de protocolos interiores de

gateways (IGP) para completar su propósito. Dicho de otra manera, el nodo fuente mapea la dirección de Internet destino en una dirección de Hardware y envía el paquete al nodo destino usando esta dirección. Estos trazados (mapeos) son normalmente realizados a través de una tabla de traslación, si el contacto (dirección) no se encuentra para una dirección destino de Internet, el ARP se involucra para determinar esta dirección. Esta forma de movilizar información en una red es también llamado ***ruteo directo.***

Los routers que mueven información entre sistemas autónomos son llamados ***exterior routers***, es decir, que los nodos de la fuente y el destino están en diferentes redes lógicas dentro de una Internet y ellos usan un protocolo exterior de gateways para este propósito. Este ruteo funciona de la siguiente manera; el nodo fuente envía paquetes hacia un gateways o router en la misma red usando el ruteo directo. Desde ahí, los paquetes son enviados a cruzar gateways o routers intermedios, como requisito, hasta que ellos lleguen a la red destino. El ruteo directo es entonces usado para enviar los paquetes hacia el host destino en esta red. Cada gateways, router y host en una Internet, tiene su propia tabla de ruteo que define la dirección que tomara la información para conducirlo a un siguiente gateway que se encuentre en otras redes dentro de una Internet. Esta forma de movilizar información en una red a otra es también llamado ***ruteo indirecto.***

La arquitectura de Internet se muestra en la siguiente figura.



Arquitectura de Internet

Los protocolos de ruteo de IP son dinámicos. En las llamadas dinámicas de ruteo para enrutar paquetes, estas pueden ser calculadas a intervalos regulares por software en los dispositivos de ruteo, esto contrasta con los ruteos estáticos, donde las rutas son establecidas por el administrador de la red y no son cambiadas hasta que el administrador las cambie, una tabla de ruteo de IP consiste de ***destination address/next hop.***

El ruteo de IP especifica que datagramas de IP viajaran a través de una Internet de trabajo un viaje a la vez, la ruta entera es desconocida al inicio del viaje. En su lugar, a cada alto (gateway, router o host), el siguiente destino es calculado por la combinación de direcciones destino dentro del datagrama con la actual tabla de ruteo del nodo, cada nodo participa en el proceso de ruteo consistiendo solo de transporte de paquetes basados en la información interna, sin considerar por las medidas de los sucesos que pueda o no alcanzar el destino final. En otras palabras, el IP no se preocupa por suministrar reportes de errores de regreso a la fuente cuando ocurren anomalías de ruteo, esta tarea es permitida por otro protocolo de Internet : el ***Internet Control Message Protocol (ICMP).***

ICMP

El ***Internet Control Message Protocol (ICMP)*** realiza un numero de tareas especificas del Internet Protocol (IP) en una Internet, la principal razón por la que fue creado es para dar reportes de apoyo de posibles fallas de ruteos para la fuente, el ICMP también provee un método para probar nodos a través de una Internet, esto es posible con el ICMP Echo y Reply Messages; un método para estimular ruteos más eficientes con el ICMP Redirect messges; un método para informar a las fuentes que un datagrama tiene excedido su tiempo asignado para existir dentro de la internet a través de el ICMP Time Exceeced message; además de otros mensajes útiles. Una característica recientemente agregada a ICMP es la de proveer una forma útil para que nuevos nodos descubran el subnet mask que actualmente esta siendo usado en una Internet.

El ICMP es una parte integral de cualquier implementación de IP, particularmente aquellas que corren en routers.

Capa de Transporte

La capa de transporte de Internet es implementada por TCP y el ***User Datagram Protocol (UDP).*** TCP proporciona conexión orientada al transporte de datos, mientras que la operación de UDP es pasar los datos por el menor numero de conexiones (nodos) posibles.

Transmission Control Protocol (TCP)

TCP proporciona una comunicación full-duplex, es el reconocedor y controlador del flujo de servicios a los protocolos de las capas superiores; como mover datos en una continua corriente de bytes sin estructura, donde los bytes son identificados por la secuencia de números, TCP también puede soportar numerosas conversaciones simultáneas con las capas superiores, el formato del paquete de TCP es mostrado en la siguiente figura.

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgment Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Flags</td><td>Windows</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="4">Options (+ padding)</td></tr>
<tr><td colspan="4">Data (variable)</td></tr>
</table>

Formato del Paquete TCP

* El campo *source port* identifica el punto en el cual un proceso de las capas superiores de una fuente en particular recibe servicios TCP; el campo *destination port* identifica el puerto destino que procesa en las capas superiores servicios TCP.

* El campo *sequence number* usualmente especifica el numero asignado al primer byte de datos en el mensaje actual, bajo ciertas circunstancias, esto puede ser usado también para identificar un numero de secuencia inicial que será usado en la próxima transmisión
* El campo *acknowledgment number* contiene el numero de secuencia del siguiente byte de datos enviados del paquete esperando ser recibidos.
* El campo *data offset* indica el numero de palabras de 32 bits en el encabezado TCP
* El campo *reserved* es reservado para usos futuros por los diseñadores de protocolos
* El campo *flag* lleva una variedad de información de control
* El campo *window* especifica el tamaño de la ventana receptora de envíos (espacio de buffers disponibles para recibir los próximos datos)
* El campo *urgent pointer* apunta el primer byte de datos urgente en el paquete
* El campo *options* especifica varias opciones de TCP

User Datagram Protocol (UDP)

Este protocolo es utilizado en algunas aplicaciones en lugar del TCP, es mucho más sencillo porque no se preocupa porque los paquetes se pierdan, ni por que la información llegue en orden o cualquier situación de este tipo, el UDP se utiliza en programas que envían mensajes cortos y que solo reenvían la información si no reciben una respuesta en un tiempo determinado.
El encabezado de UDP solo tiene cuatro campos: *source port, destination port, lenght,y UDP checksum;* los campos source y destination port desempeñan las mismas funciones tal como la realizan en el encabezado TCP, el campo lenght especifica la longitud del encabezado UDP y los datos, y el campo checksum permite verificar la integridad de los paquetes y es opcional.

Protocolos de las Capas Superiores

Como fue mencionado anteriormente, el protocolo de Internet incluye muchos protocolos que en las capas superiores representan una gran variedad de aplicaciones, incluyendo la administración de la red, la transferencia de archivos, servicios de distribución de archivos, emulador de terminal y correo electrónico. La figura muestra los protocolos de las capas superiores de Internet con la aplicación que ellos soportan.

Aplicación	Protocolos
File Transfer	FTP
Terminal Emulation	Telnet
Electronic Mail	SMTP
Network Management	SNMP
Distribuited File Services	NFS, XDR,RPC X Windows

Tabla de Internet, Protocolos/Aplicación

El *File Transfer Protocol (FTP)* proporciona una forma de mover archivos entre sistemas de computadoras. *Telnet* permite una emulación de terminal virtual. El *Simple Network Management Protocol (SNMP)* es un protocolo de administración de red usado para reportar condiciones de anomalías en la red y valores al principio del ambiente de red. *X Windows* es un popular protocolo que permite a terminales inteligentes comunicarse con computadoras remotas como si estas estuvieran adheridas a sus monitores. *Network File System (NFS), Externa Data Representation (XDR) y Remote Procedure Call (RPC),* todos ellos combinados, permiten el acceso transparente a recursos remotos de red. El *Simple Mail Tranfer Protocol (SMTP)* proporciona un mecanismo de transporte de correo electrónico. Estas y otras aplicaciones de red usan los servicios de TCP/IP y otros protocolos de Internet en las capas bajas, para proveer a los usuarios servicios básicos de red.

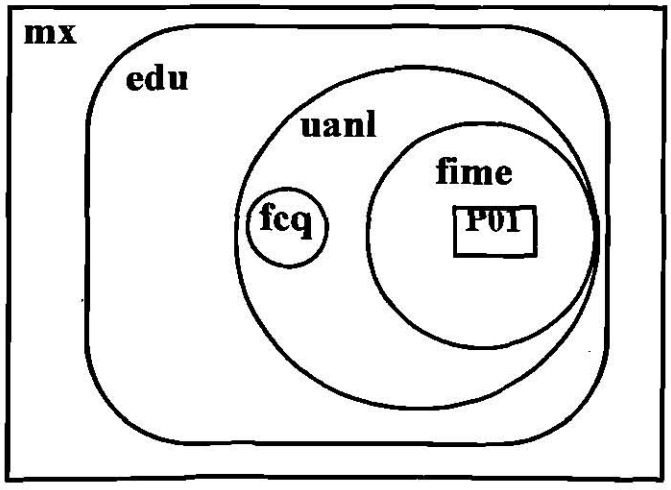
Sistema de Nomenclatura de Dominios

Al principio, la gente aceptaba que las combinaciones de números como domicilios estaba bien para que las maquinas se comunicaran entre si, pero las personas prefieren utilizar nombres, por eso a las computadoras de Internet se le asignaron nombres para la conveniencia de los usuarios. Al principio cuando Internet no tenia la cantidad de usuarios como ahora el manejo de los nombres era sencillo, por eso el NIC, Centro de Información de la Red (Network Information Center), estableció un registro, este registro se llama *Sistema de Nomenclatura de Dominios* que distribuye en diferentes grupos la responsabilidad de subconjuntos de nombres. A cada nivel de este sistema se le llama *dominio* y se separan por puntos :

ux.cso.uiuc.edu

p01.fime.uanl.edu.mx

Puede haber cualquier cantidad de dominios en un nombre, pero en muy raras ocasiones se verán nombres con más de cinco. Al leer el nombre de izquierda a derecha, cada dominio será más vasto que el dominio que tenga a la izquierda. En el nombre **p01.fime.uanl.edu.mx**, **p01** es el nombre del equipo anfitrión, una computadora con un dominio IP (ver figura). El nombre para esta computadora se asigna y mantiene por el grupo **fime**, que es el departamento donde esta se localiza, este departamento **fime** es parte de la Universidad Autónoma de Nuevo León **uanl** que esta en un grupo nacional de instituciones educativas **edu** en el país de México **mx**, el dominio **uanl.edu.mx** contiene a todas las computadoras de la Universidad Autónoma de Nuevo León y así sucesivamente.



Autoridad sobre dominios

Es fácil saber cuando los nombres vienen de una organización como una universidad o un negocio pues se crearon dominios de jerarquía superior como **edu**, originalmente existían seis dominios ver figura.

Dominio	**Utilización**
com	Para organizaciones comerciales (negocios)
edu	Organizaciones educativas (Universidades,sec.,etc.)
gov	Organizaciones gubernamentales sin incluir la milicia
mil	La milicia
net	Recursos de la Red

Cuando Internet se convirtió en una red internacional, se requería que los países tomaran la responsabilidad de sus propios nombres, por eso existe un conjunto de dominios de dos letras que corresponden a los países por ejemplo:

au Australia
ca Canadá
fr Francia
mx México
uk Reino Unido
us Estados Unidos.

Aplicaciones

TELNET

Es el protocolo de sesión de trabajo remota de Internet, nos permite estar frente al teclado de una computadora y establecer una sesión en una computadora remota en la red. La sesión puede ser una maquina en la misma oficina, en la universidad o en el otro lado del mundo, cuando nos conectamos es como si el teclado estuviera conectado a otra computadora remota. Se podrá tener acceso a todos los servicios que esa maquina provee a sus terminales locales, se puede hacer una conexión interactiva normal (conectándose y tecleando comandos) o tal vez tener acceso a muchos servicios especiales, como buscar en algún catalogo de biblioteca, saber que esta pasando en Peoría, tener acceso al texto del periódico USA Today y aprovechar muchos de los servicios disponibles en los diferentes equipos de red.

La forma más sencilla de usar **telnet** es teclear :

% **telnet** *domicilio-Internet-de-computadora-remota*

en el nivel de comandos, se esta empleando la cápsula C de los sistemas UNIX, por lo que el indicador es un signo de porcentaje (%). Si se usa otro sistema operativo en la computadora (como DOS, VAX/VMS o una Macintosh), el comando seria fundamentalmente el mismo, con la excepción de algunos detalles pequeños que pueden ser distintos. A continuación se presenta un ejemplo básico :

% telnet p01.fime.uanl.edu
Trying ...
Connected to p01.fime.uanl.edu
Escape character is '^'
SunOS UNIX (sonne)
Login : **krol** ***identificándose en el sistema remoto***
password : ***la contraseña no se ve***
Last login : Sat Sep 7 17:16:35 from p02.fime.uanl.edu
SunOS Release 4.1 (GENERIC) #1
Sonne% **ls** ***comando que se ejecuta por el sistema remoto***
Mail News development project1
Sonne% **logout** ***desconexion del sistema remoto***
% ***de nuevo esta en el sistema local***

En este ejemplo se pidió a TELNET que encontrara una computadora llamada **p01.fime.uanl.edu**. Después de encontrarla, se inicia la sesión de terminal, una vez que inicia la sesión, el dialogo que se da aparenta ser el mismo que el de una terminal conectada directamente a esa computadora.
Esto es realmente TELNET : una herramienta que le permite establecer una sesión en sistemas remotos.

FTP

Este comando recibe el nombre de **ftp** debido al protocolo de aplicación que usa: el Protocolo de Transferencia de Archivos (FTP: File Transfer Protocol). Como su nombre lo indica, la función del protocolo es mover archivos de una computadora a otra. No importa donde estén estas computadoras, como estén conectadas o si tienen o no el mismo sistema operativo, dado que ambas computadoras "hablan" el protocolo FTP y tienen acceso a Internet, es posible utilizar el comando **ftp** para transferir archivos. Algunas de las características de su uso cambian con cada sistema operativo, pero la estructura básica de comandos es la misma en cualquier maquina.
Para mover archivos entre dos computadoras en las cuales ya se tiene una cuenta **ftp** requiere que se especifique la maquina de la cual se quiere extraer los archivos. Esto se hace con el comando siguiente:

% **ftp** Nombre-de-la-maquina-remota.

Este comando inicia el programa **ftp** y conecta al usuario a la maquina especificada. Cuando **ftp** efectúa la conexión con la computadora remota, solicitara al usuario que se identifique dando una identificación y una contraseña:

% ftp p01.fime.uanl.edu
Connected to p01.fime.uanl.edu
220 sonne FTP server (SunOS 4.1) ready.
Name (ux.uiuc.edu:krol): **krol** ***Enviando la clave de usuario krol***
331 Password required for krol.
Password: ***La contraseña no se vera en pantalla***
230 User krol logged in.

Con algunos sistemas operativos como DOS y Macintosh, **ftp** puede no solicitar una contraseña, es posible que solo se necesite una clave de usuario

dado que no hay seguridad de contraseñas en el sistema. En esas máquinas, la protección contra el acceso no deseado es manejada deshabilitando el software del servidor FTP.
La clave de usuario que se utiliza determina a que archivos se tiene acceso, de la misma manera que si se estuviera conectado localmente. Sin embargo, recuerde que deberá teclear una clave y una contraseña apropiadas para poder entrar al sistema remoto. Una vez que el sistema remoto acepta la cuenta y la contraseña, se encuentra listo para empezar a transferir archivos, **ftp** despliega ftp> como indicador para recibir comandos; puede transferir archivos en dos direcciones. Es posible tomar un archivo de la maquina local (la que inicia la transferencia) y colocarlo (**put**) en la maquina remota, o extraerlo (**get**) y colocarlo en la maquina local. Los comandos **get** y **put** tienen la sintaxis siguiente:

ftp> **get** archivo-fuente archivo-destino
ftp> **put** archivo-fuente archivo-destino

Archivo fuente es el nombre del archivo existente (el archivo que se quiere copiar) y *archivo destino* es el nombre de la copia recientemente creada, si se omite se asigna el nombre del archivo-fuente a la copia.
En el siguiente ejemplo, se hará una conexión a la maquina **ux.uiuc.edu** con el nombre **boss**, se transferirá el archivo *comments* localizado en el directorio de la cuenta **krol**, de la maquina **p01.fime.uanl.edu.** Después se transferirá el archivo *newversion* a **p01.fime.uanl.edu**, asignándole el nombre *readthis* a la copia nueva:

ux login: **boss** ***Se envía la clave de usuario boss a ux***
password: ***No aparece en pantalla lo tecleado***

Welcome to ux.uiuc.edu

ux% **ftp p01.fime.uanl.edu**
Connected to p01.fime.uanl.edu.
220 fime FTP server (SunOS 4.1) ready.
Name (ux.uiuc.edu: boss) : **krol** ***Se envía la clave de usuario krol***
331 Password required for krol
Password: ***No aparece en pantalla lo tecleado***
230 User krol logged in.
ftp> **get comments** ***Se solicita la copia del archivo comments***
200 PORT command successful ***Se desplaza el archivo de fime a ux***

150 ASCII data conection for comments (128.174.5.55,3516)(1588bytes)
226 ASCII transfer complete
1634 bytes received in 0.052 seconds (30 kbytes/s).
ftp> **put newversion readthis** ***Se copia newversion de ux a fime***
200 PORT command successful ***Se renombra con readthis***
150 ASCII data conection for readthis (128.174.5.55,3518)
226 ASCII transfer complete.
62757 bytes sent in 0.22 seconds (2.8e+02 kbytes/s)
ftp> **quit** ***Finaliza la sesión***
221 Goodbye.
ux%

Es importante saber como salirse del programa y también como entrar, cuando se termine de transferir los archivos, se teclea el comando **quit** para terminar la ejecución del programa **ftp**, el comando **bye** hace lo mismo.

SMTP

Simple Mail Transfer Protocol (SMTP) es un protocolo de correo electrónico con funciones tanto para el cliente y el servidor.
El correo electrónico (o email) es la aplicación más frecuente para que la gente se comunique en las redes de computadoras en la forma más rápida posible, como una conversación normal. Esto permite a la gente escribir de aquí para allá sin dedicar mucho tiempo inquietante acerca como el mensaje obtenido actualmente será entregado, el correo electrónico es dependiente acerca del concepto de una dirección. Nuestra dirección de **email** proporciona toda la información requerida para obtener un mensaje para nosotros desde cualquier parte del mundo.
Una dirección no necesariamente tiene que ser para una persona en particular, las direcciones de **Email** usualmente aparecen en una de las dos formas, usando el formato de Internet que contiene un signo "at", '@' , o usando el formato UUCP que contiene el punto de exclamación'!', también llamado como "bang". A manera de ejemplo si una persona, digamos Adrián Hernández, contara con una cuenta en la red de la Universidad Autónoma de Nuevo León, esta tendría el siguiente formato: Ahdz@ccr.dsi.uanl.mx..

Otro símbolo que entra en esta parte es %, actuando como un método extra de routing. Para ejecutar el programa **mail** hay que dar el comando :

% **mail** cadena_de_domicilios

El parámetro *cadena_de_domicilios* es opcional, si se proporciona ahí el comando envía un mensaje a las personas listadas en el conjunto de domicilios, normalmente se pueden usar espacios o comas para separar los domicilios listados, si no hay una lista de domicilios, **email** entra en el modo de comandos, una de las cosas que se pueden hacer en el modo de comandos es leer los mensajes recibidos.

TCP/IP cuenta con una gran variedad de protocolos, el propósito de esta tesina es mostrar en parte dicho protocolo pero este cuenta con más, que solo mencionare como es el ***Network News*** que es el equivalente en Internet a los grupos de discusión o el tablero de foros de discusión (BBS), otro es ***Archie*** que nos sirve para encontrar archivos, también están los ***Gopher*** que es una herramienta para ayudar a buscar y tener acceso a una gran variedad de recursos en línea, y por ultimo cuenta también con el ***WWW*** que es un intento de organizar toda la información en Internet, además de cualquier otra información local que se necesite.

La siguiente tabla muestra algunos de los protocolos más comunes dentro del conjunto de protocolos de TCP/IP y el servicio que proporcionan :

PROTOCOLO	SERVICIO
Internet Protocol (IP)	Proporciona servicios de entrega de paquetes entre nodos.
Internet Control Message Protocol (ICMP)	Control de Errores y Mensajes entre equipos "hosts" y "gateways"
Address Resolution Protocol (ARP)	Convierte direcciones Internet a direcciones Físicas
Reverse Address Resolution Protocol (RARP)	Convierte direcciones Físicas a direcciones Internet

Transmission Control Protocol (TCP)	Proporciona entrega de datos confiable entre clientes
User Datagram Protocol (UDP)	Proporciona entrega de paquetes en una forma no muy confiable, y sin establecer una conexión entre clientes
File Transfer Protocol (FTP)	Proporciona servicios a nivel aplicación, para trensferencia de Archivos
Telnet	Proporciona Emulación de Terminal

A continuación se listan algunos ejercicios básicos de configuración utilizando el software de TCP/IP llamado PC-TCP.
Antes de poder trabajar con el software es necesario instalar la tarjeta de comunicaciones que será utilizada y además, configurar los parámetros necesarios :

Parámetros de Hardware :
Base I/O Address
Base Memory Address
DMA Channel
Interrupt Vector (IRQ)

Parámetros de Software :
Controlador de Dispositivo correspondiente a la tarjeta usada.
Direcciones Internet de nodos y servidores en la red

- Prueba de Comunicación :
Para ejecutar esta prueba es necesario conocer la dirección Internet de un equipo remoto que este ejecutando el software de TCP/IP.
Ejecutar el comando :
comando ping hostname
hostname : es la dirección del equipo con el que se desea establecer la comunicación

Después de esto se despliega una pantalla de estadísticas acerca de la conexión. Si todo esta correcto, en las primeras líneas aparecerá el mensaje: Host Responding. Si se tuvo algún error el program "ping" informara sobre el problema con un mensaje similar a los siguientes : "Host not responding" o "Host Unreachable".

- Establecer una sesión de Terminal Virtual
Comando : tn hostname

- Efectuar una Transferencia de Archivos
Comando : ftp hostname

Sistema de Archivos Distribuido : NFS

NFS (Network File System), desarrollado por SUN MICROSYSTEMS INC., como un herramienta para redes "MULTIPROVEEDOR". Proporciona acceso a archivos remotos, a través de TCP/IP, permitiendo accesar archivos localizados en directorios de maquinas remotas. Aunque NFS puede en teoría ser implementado para otros protocolos , actualmente es encontrado principalmente para sistemas que utilizan TCP/IP, como los siguientes : SCO UNIX, PCs, VAX VMS, HP/UX, SEQUENT/DYNIX e IBM AIX.
NFS tiene dos protoclos asociados con el. Estos son RPC (Remote Procedure Call) y XDR (External Data Representation). Estos protocolos implementan los niveles OSI "SESSION" y "PRESENTATION" respectivamente.

RPC proporciona al usuario una manera simple de implementar llamadas de procedimientos hacia otros sistemas. Maneja envío de parámetros y recibe valores de retorno de funciones.

XDR permite especificar tipos de datos dependientes del procesador, los cuales son consistentes a través de la red. Por ejemplo, una cadena de caracteres o números de punto flotante pueden ser implementados usando patrones diferentes de bits en dos diferentes rutinas.

Actualmente más de 290 organizaciones tienen licencia de NFS, y aproximadamente la mitad de estas, son licencias comerciales.
Para permitir compartir archivos, NFS establece al sistema de archivos de UNIX como un drive virtual en la PC. Este drive virtual funciona como un canal del ambiente DOS al ambiente UNIX. Esto es, el sistema de archivos de UNIX aparece a la PC como un drive d:. Los archivos que residen el equipo UNIX, pueden ser accesados como si estuvieran en disco duro local de la PC.
Se pueden copiar archivos hacia y desde el drive virtual como se copiaría un archivo desde un floppy en el drive a:.
A diferencia de un file transfer, NFS permite al usuario trabajar con un archivo remoto sin tener que hacer un copia de este archivo a hacia su sistema local. Este método de compartir archivos tiene muchas ventajas.
Debido a que existe solo una versión de un archivo, los usuarios se evitan la confusión que pudiera ocurrir cuando más de una persona esta trabajando en un proyecto, y dos de ellos efectúan cambios a multiples copias del mismo archivo. Todavía más, los archivos pueden fácilmente ser respaldados por el administrador del sistema.
Bajo NFS, los archivos almacenados en el disco virtual de la PC (en realidad es el sistema de archivos de UNIX), pueden ser accesados por otros usuarios sin importar si ellos están utilizando terminales conectadas al sistema UNIX, u otras PC conectadas vía NFS. Por supuesto que para mantener la seguridad requerida en un sistema multiusuario, todos los archivos del disco virtual, son protegidos con los permisos de acceso a archivos propios de UNIX.
Otra característica bastante relevante, es que las aplicaciones dos pueden ser almacenadas en el disco UNIX, y accesadas desde la PC como si estuvieran residentes en un disco local. Así mismo, los usuarios de la PC pueden usar archivos UNIX para aplicaciones DOS. Por ejemplo, un usuario de PC puede accesar información almacenada en un sistema manejador de base de datos multiusuario.
Un pequeña complicación, es que los nombres de archivos y formato de archivos de DOS y de UNIX difieren ligeramente. Sin embargo existe software
para compensar estas diferencias.
En resumen, NFS ofrece acceso a archivos, en lugar de las facilidades de file transfer que se pueden encontrar en programas de comunicación serial (por ejemplo, emuladores de terminal).

Algunas versiones de NFS y TCP/IP son :

PC-NFS	SUN MICROSYSTEMS
PC/TCP	FTP SOFTWARE
AXCESS	ATLANTIX
POWERFUSION	PERFORMANCE TECHNOLOGY's
PATHWAY	THE WOLLONGONG GROUP
CU/TCP	CLARKSON UNIVERSITY

Bibliografía

TCP/IP, ISO and Multivendor Networking, Datapro, May 90.
An Overview of UNIX Communications, Datapro, ago 90.

Conéctate al mundo de Internet, De Krol, O'reilly & Associates.

Departmental Strategy, Datapro, May 90.

Linking LANs, Schatt, McGrawHill.

Redes de Ordenadores, Tanenbaum, Prentice Hall.

ARPA .- es un estándar de facto diseñado por el departamento de la defensa de los E.U. para enlazar computadoras de distintos proveedores, trabajando con sistemas operativos diferentes.

ARPANET.- es una red "MULTIVENDEDOR" implementada por el departamento de la defensa de E.U. para apoyar proyectos de defensa.

ISO .- (International Organization for Standarization)
Organización Internacional para Estandarizacion.

OSI .- (Open Systems Interconection)
modelo de interconexión de sistemas abiertos para arquitecturas de red.