16
2q.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS
A R A G Ó N

" TCP / IP - INTERNET "

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

ESPADAS RESENDIZ JAVIER

ENEP ARAGON

MEXICO, D.F. [redacted]

1997

DEDICATORIA:

Para mis hermanos:

Emma
Elvira
Fernando
Marcos
Adolfo
Obdulia
Ricardo
Juana

A mi Madre:

Jovita Reséndiz Aranda

Y muy en especial a:

Marisela Saldaña Contreras

CONTENIDO

	Página
INTRODUCCIÓN	**1**
CAPITULO I. ANTECEDENTES.	
I.1. Orígenes y concepto de Internet.	**3**
I.2. Funciones principales de las organizaciones Internet.	**6**
I.3. Que es TCP/IP.	**8**
I.4. Conceptos de TCP/IP.	**10**
I.4.1. Modelo OSI.	**10**
I.4.2. Analogía entre el modelo OSI y TCP/IP.	**17**
I.5. Modelo TCP/IP.	**18**
I.5.1. Comparación entre modelo OSI y TCP/IP.	**20**
I.6. El protocolo TCP/IP.	**24**
CAPITULO II. DIRECCIONAMIENTO.	
II.1. Identificadores universales.	**27**
II.1.1. Direccionamiento IP.	**28**
II.1.2. La necesidad de manejar direcciones.	**28**
II.1.3. Características de las direcciones IP.	**29**

Página

II.1.4. Formato y componentes de la dirección IP. 31
II.2. Clases de direccionamiento. 32
II.2.1. Números de red y números de host. 33
II.2.2. Distinguiendo la clase de dirección. 36
II.2.3. El IAB y el registro del número de red. 38
II.2.4. Ventajas y desventajas de la inscripción. 42
II.3. Dirección especifica de la red. 43
II.3.1. El sistema nombre de dominio. 43
II.3.2. Eligiendo un esquema nombre de dominio. 45
II.4. Sistema autónomo. 48
II.4.1. Números del sistema autónomo. 49
II.4.2. Cómo elegir su propio número de red. 50
II.4.3. Direcciones IP reservadas. 52
II.5. Acceso a Internet en México. 54

CAPITULO III. PROTOCOLOS DE TRANSPORTE.

III.1. Las facilidades de IP. 56
III.1.1. Encapsulamiento. 58
III.1.2. Fragmentación, reensamble y la unidad de transferencia máxima. 59
III.2. Direccionamiento IP. 60

Página

III.2.1. Tipo de servicio. **61**
III.2.2. El datagrama IP. **63**
III.2.3. Fragmentación y reensamble. **71**
III.3. Protocolos. **74**
III.3.1. Protocolo de resolución de dirección. **74**
III.3.1.1. Formato ARP. **77**
III.3.1.2. ARP en operación. **79**
III.3.2. Protocolo de resolución de dirección inverso. **80**
III.3.3. Protocolo de mensajes de control Internet. **82**
III.4. Protocolos del nivel de transporte. **84**
III.4.1. Puertos. **86**
III.4.2. Sockets. **88**
III.4.3. Protocolo de datagrama de usuario (UDP). **90**
III.4.4. Protocolo de control de transmisión (TCP). **92**
III.4.5. TCP. **94**
III.4.5.1. El encabezado TCP. **94**
III.4.5.2. TCP en acción. **101**
III.4.5.2.1. Fase de conexión. **101**
III.4.5.2.2. Fase de datos. **103**
III.4.5.2.3. La fase final. **108**
III.4.6. Corrección de errores y retransmisión time-out. **110**

Página

III.4.7. Ventanas de deslizamiento, ventana de avisos y control de flujo. **115**

CAPITULO IV. APLICACION.

IV.1. Modelo cliente/servidor. **120**

IV.2. Aplicaciones en TELNET, FTP, SMTP Y X WINDOWS. **122**

IV.2.1. TELNET. **122**

IV.2.2. El papel DE TELNET. **123**

IV.2.3. Protocolo de transferencia de archivo FTP. **125**

IV.2.4. Protocolo simple de transferencia de correo SMTP. **129**

IV.2.5. Protocolo X. **131**

IV.3. Sistema de administración de red. **134**

CONCLUSIONES **138**

BIBLIOGRAFÍA **142**

INTRODUCCIÓN.

Las primeras redes de computadoras se construyeron alrededor de un procesador central, haciendo relativamente fácil para los usuarios el usar archivos compartidos. A finales de los 70´s con el advenimiento de las computadoras, las compañías con más de un computador ofrecían a sus usuarios puertos de acceso a terminales para cada minicomputador. Solamente a fines de los 80´s, cuando proliferaron las computadoras personales (PC's) y las redes de área local (LAN's), se comenzó a manejar la información de manera aislada, surgiendo así una gran necesidad de interconexión. La búsqueda ardua para encontrar algún camino que permitiera a estas islas de información comúnmente llamadas grupos de trabajo, compartir archivos, aplicaciones y otros trabajos relacionados, trajo consigo una serie de productos dispuestos a librar los obstáculos.

Muchos grupos han esperado a que el modelo OSI resuelva un sinfín de problemas para la interconexión de redes con computadoras de diferentes proveedores. Pero conforme los 80's fueron pasando, se fue terminando para muchos el sueño de OSI que tenían desde hace muchos años.

Con la lenta caída del despliegue OSI, se esperarían nuevas estrategias de conexión, y al inicio de los 90's TCP/IP comenzó a tener un incremento notable de usuarios, vendedores y soportes en general. Mientras que TCP/IP puede no tener todo el grupo de funciones de OSI, tiene sin embargo, un buen grupo de

funciones tales como un estándar abierto, una buena base para su producto, soporta manejadores de red estándar y es el que hoy en día está disponible.
El presente trabajo tiene la finalidad de mostrar de una manera clara el protocolo TCP/IP como una herramienta que permite la interconexión de redes de diferentes plataformas, sin entrar a detalles propios de aplicaciones y/o programación.

El primer capítulo presenta una serie de antecedentes, desde el origen de las redes de comunicaciones hasta el surgimiento de la red internet.

Como se tratará en el contenido del texto, el direccionamiento internet juega un papel fundamental para lograr la interconexión entre redes que utilizan estos protocolos. El capitulo 2 presenta un estudio amplio sobre el direccionamiento en internet.

El capitulo 3 condensa los principales conceptos, características y partes que componen los protocolos TCP/IP.

En el capitulo 4 se describen algunas de las aplicaciones más importantes de estos protocolos y cómo impactan a la comunicación entre redes.

El trabajo concluye con los aspectos más relevantes sobre las futuras direcciones que TCP/IP e internet pueden tomar y su impacto en la interconexión de redes; las limitaciones de TCP/IP y un plan de migración de estos protocolos hacia OSI.

I. ANTECEDENTES.

I.1. ORÍGENES Y CONCEPTO DE INTERNET.

La comunicación de datos ha llegado a ser una parte fundamental de la computación. En todo el mundo las redes de computadoras acumulan datos sobre diversos elementos como las condiciones atmosféricas, la producción de granos y el tráfico aéreo entre otros. Ciertos grupos tienen establecido un correo electrónico con el que pueden conseguir información de interés común. En el mundo científico las redes de datos son esenciales porque permiten a los usuarios enviar programas y datos a las supercomputadoras remotas para su procesamiento, captura de resultados e intercambiar información científica.

Desafortunadamente, muchas de estas redes son entidades independientes, establecidas para satisfacer las necesidades de un grupo en particular. Si estos grupos desean comunicarse entre sí, tienen que elegir una tecnología adecuada que les ayude a resolver sus problemas de comunicación.

Actualmente el intercambio de información a grandes distancias se ha vuelto un factor determinante en el desarrollo social. La informática y las telecomunicaciones son las herramientas que demandan los grandes usuarios por la gran cantidad de datos que generan.

Como una solución al problema, surgió una tecnología de interconexión que hizo posible que diferentes redes se interconectaran como una unidad coordinada. Esta nueva tecnología se llamó **Red Internet**.

Es conveniente aclarar que existe muy probablemente, una confusión de términos entre el significado de internet (con " i " minúscula) e Internet (con " I " mayúscula). Pero la diferencia es muy simple. Una internet es cualquier interconexión de redes y una Internet se refiere a una conjunción de redes, con características propias de interconexión, direccionamiento, protocolos de comunicación y reguladas por un organismo central, como se muestra en la figura 1.1.

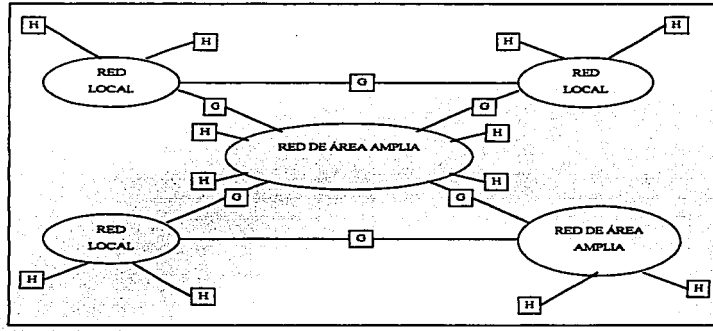

Fig. 1.1. Ejemplo de configuración Red Internet

Internet es una red de amplia cobertura, de comunicación de paquetes, que emplea el protocolo TCP/IP y soporta servicios de computo en ambientes de ingeniería, investigación, educación y comercial.

La Red Internet al tener una base tan grande a nivel mundial cuenta con objetivos muy claros y específicos para facilitar la posibilidad de compartir recursos entre las organizaciones participantes como agencias de gobierno, instituciones educativas y corporaciones privadas, así como promover el interés y participación de investigadores y proveerles de un ambiente de prueba para nuevos desarrollos en redes de comunicación.

Red Internet.

Su origen se remonta a la creación de una red de comunicaciones desarrollada por el gobierno de los Estados Unidos.

A principios de los 70's, el Departamento de Defensa (DoD) encargó a la Agencia de Proyectos e Investigación Avanzada (ARPA) el desarrollo de un conjunto de protocolos de comunicaciones, denominado TCP/IP.

Inicialmente se conectaron 3 universidades y un centro de investigaciones empleando dicho protocolo para conformar la red ARPANET.

Esta creció en forma acelerada debido a que los programas fuente del protocolo de comunicaciones se hicieron del dominio público por lo que los diferentes fabricantes incorporaron TCP/IP en sus equipos.

ARPANET fue la primera red de paquetes que permitió conectar computadoras heterogéneas, esto es, computadoras de diferentes tipos que por primera vez se comunicaron para intercambiar información, gracias a los protocolos de red desarrollados.

En un principio no fue considerada una internet debido a que interconectaba nodos más no redes.

Al ir incorporando más nodos a la red ARPANET, el DoD decidió separarla administrativamente en dos partes: ARPANET para propósitos de investigación y MILNET, para comunicación militar.

Hoy en día la Red Internet está conformada por redes distribuidas en todo el mundo, tales como NSFNET, NSN, USENET, etc.

I.2. FUNCIONES PRINCIPALES DE LAS ORGANIZACIONES INTERNET.

A pesar de su magnitud, no existe una autoridad central que defina criterios para el manejo de Internet, pues se encuentra integrada por diversas redes

independientes que forman una red cooperativa, cada una de ellas con una administración propia, así como políticas, reglas y procedimientos particulares.

Internet es coordinada por un organismo dependiente de DoD, Centro de Información de Redes (DDN-NIC), operado por SRI International, en Menio Park, California y por el Centro de Operación de Redes (NOC), en Cambridge, Masachusetts. Fig. 1.2.

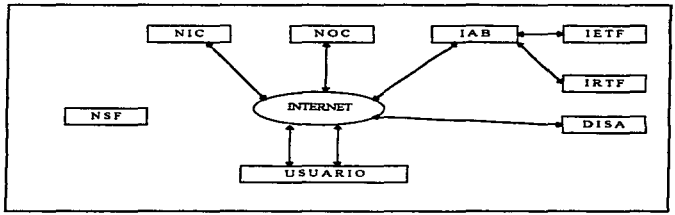

Fig. 1.2. Organización de Internet.

Sin embargo, ciertas agencias gubernamentales han sido partícipes en el establecimiento de las políticas que se siguen en Internet. En estos momentos, las decisiones políticas importantes provienen de la Fundación Nacional de Ciencia (NSF) y Agencia de Sistemas de Información de Defensa (DISA).

Las innovaciones técnicas que permiten que esta red mantenga una alta calidad en sus servicios, usualmente se trabajan con la comunidad técnica bajo los auspicios de un grupo llamado Comité de Actividades Internet (AIB) y sus grupos de trabajo, donde se analizan los problemas técnicos y desarrollan

soluciones, las cuales son puestas a consideración de la comunidad Internet y el IAB para que sean implantadas. La implantación de nuevas normas, depende de la cooperación y recursos de cada nodo Internet, ya que no existe un mecanismo que obligue a un nodo a implantar una nueva norma.

El IAB está integrado por dos grupos de trabajo: el Grupo de Ingeniería de Internet (IETF) y el Grupo de Investigación de Internet (IRTF).
El IRTF promueve la investigación y el desarrollo de nuevas tecnologías de redes de comunicación.

I.3. QUE ES TCP/IP.

El nombre más común para el grupo de protocolos que se van a describir es "La familia o *suite* de protocolos de INTERNET". TCP e IP forman parte del conjunto de protocolos interrelacionados.

Se le llama *suite* porque en sistemas complejos de comunicación de datos, no es factible usar un protocolo sencillo para manejar las tareas de transmisión, requiriéndose así un grupo de protocolos los que cooperando entre sí, eviten problemas comunes tales como fallas de hardware, congestión en la red, retardo o pérdida de paquetes, corrupción de datos y errores en secuencia o duplicación de datos.

La función de TCP/IP es permitir que dos procesos o programas de aplicación se comuniquen a través de una Red Internet.

Debido a que TCP e IP son los protocolos de transporte más conocidos, se ha vuelto común usar el término TCP/IP para referirse a toda la familia.

La mayoría de las redes que engloba Internet se comunican mediante el protocolo **TCP/IP (Transmission Control Protocol / Internet Protocol ó Protocolo de Control de Transmisión / Protocolo de Inter-red).**

El principal acierto del protocolo fue el haber desarrollado una arquitectura de comunicaciones sólida en caso de que la red o sus componentes sufrieran fallas, además de que puede acomodar múltiples servicios de comunicación sobre una gama de redes.

A mediados de los 80's, el protocolo se volvió muy popular en la comunidad comercial y es uno de los más utilizados. Actualmente TCP/IP está disponible para soportar desde computadoras personales hasta supercomputadoras.

Algunas aplicaciones del protocolo TCP/IP son:

- **Transferencia de Archivos**. El protocolo para transferencia de archivos (FTP) permite mover el archivo de una computadora remota a una local, aunque cada computadora tenga un sistema operativo y formato de almacenamiento diferente. Los archivos pueden ser de cualquier tamaño y pueden contener: datos, programas, reportes, etc.. La seguridad se logra solicitando al usuario su nombre y contraseña en la computadora remota.

- **Login Remoto**. El protocolo de acceso remoto para terminal de red, permite que un usuario local pueda conectarse a una computadora que se encuentre en un lugar remoto dentro de Internet. Una vez conectada y establecida la sesión con el nodo remoto, el usuario puede ejecutar programas, capturar datos ó hacer cualquier otra operación como si el nodo remoto fuera uno local. La sesión remota se inicia especificando la computadora a la que se desea conectar. Y desde ese momento hasta el final de la sesión, todo lo que es tecleado es enviado a la otra computadora.

- **Correo Electrónico**. Este permite enviar mensajes a usuarios de otras computadoras remotas. Originalmente, se utilizaban una o dos computadoras especificas, y se almacenaban "archivos de correo" en esas máquinas. El sistema de Correo Electrónico es simplemente una manera que permite incluir mensajes en el archivo de correo de algún otro usuario. La mayoría de los usuarios tienen un buzón personal de correo donde todos los mensajes recibidos se almacenan.

I.4. CONCEPTOS DE TCP/IP.

I.4.1. MODELO OSI.

Los protocolos de comunicaciones se pueden describir en capas ó niveles. Esto divide el enorme problema de cómo transferir información entre dos o más dispositivos, haciendo piezas más pequeñas y manejables las cuales pueden ser fácilmente entendidas. Si la funcionalidad de cada nivel se puede describir

exactamente, se podrán construir fácilmente sistemas que sean totalmente compatibles. El modelo que resulta de la combinación descrita de niveles, es comúnmente llamado Pila de Protocolos.

En 1977, la Organización Internacional de Estándares (International Organization for Standarization, **ISO**) comenzó a desarrollar una arquitectura de comunicaciones la cual llegaría a ser un estándar internacional, un grupo de protocolos de comunicaciones conocido cono Interconexión de Sistemas Abiertos (Open Systems Interconnection, **OSI**). Esta iniciativa tuvo el mismo propósito general que TCP/IP -intercomunicación e interoperación a través de arquitecturas de computación de diferentes fabricantes - pero a diferencia de TCP/IP, apegándose a un grupo publicado de estándares internacionales "abiertos".

La Organización Internacional de Estándares y el Comité Consultivo Internacional de Telefonía y Telegrafía (Consultative Commitee on International Telephony and Telegraphy, **CCITT**) desarrollaron el modelo de referencia llamado interconexión de Sistemas Abiertos (**OSI**) para definir redes estratificadas y protocolos con varios niveles.
El modelo de referencia OSI tiene 7 niveles. Su estructura se muestra en la Fig. 1.4.

Los objetivos que persigue este modelo son:

- Proporcionar una serie de normas para la comunicación entre sistemas.

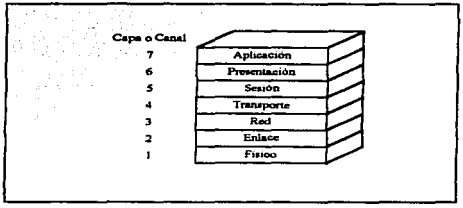

Fig. 1.4. Modelo de Referencia OSI.

- Eliminar todos los impedimentos técnicos que pudieran existir para la comunicación entre sistemas.

- Abstraer el funcionamiento interno de los sistemas individuales.

- Definir los puntos de interconexión para el intercambio de información entre sistemas.

- Limitar el número de opciones para incrementar la posibilidad de comunicación sin necesidad de costosas conversiones y traducciones entre diferentes productos.

- Ofrecer un punto de partida válido, desde el cual comenzar en caso de que las normas del estándar no satisfagan todas las necesidades.

De una manera general, a continuación se describen las características de cada una de las capas ó niveles del modelo OSI:

Nivel 1 ó Físico.

- Especifica la interconexión física, incluyendo las características eléctricas de voltaje y corriente.

- Activa, mantiene y desactiva un circuito físico entre un equipo terminal de datos (**DTE**) y un equipo de comunicación de datos (**DCE**).

Nivel 2 ó de Enlace.

- Es responsable de la transferencia de datos por el canal.

- Proporciona la sincronización necesaria para delimitar el flujo de bits del nivel físico.

- Garantiza que los datos lleguen sin errores al receptor.

- Controla el flujo de datos para impedir que el DTE se desborde en algún momento.

- Detecta errores en la transmisión y recupera los datos perdidos, duplicados o erróneos (entre nodos)

Nivel 3 ó de Red

- Define la funcionalidad de la interacción entre el DTE y la red.
- Define la unidad básica de transferencia a través de la red e incluye los conceptos de dirección de destino y enrutamiento.
- Responde a los problemas de congestión de la red.
- Especifica las opciones de encaminamiento por la red.
- Especifica la comunicación entre distintas redes.
- En este nivel está incluida la especificación X.25.
- Define la interfase entre el DTE del usuario y la red de conmutación de paquetes.
- Define la interfase entre un DTE y otro a través de la red de conmutación de paquetes.

Nivel 4 ó de Transporte.

- Proporciona la interfase entre la red de comunicación de datos y los 3 niveles superiores

- Permite al usuario elegir opciones de calidad dentro de una misma red (nivel de red).

- Asegura la transferencia de la información de extremo a extremo.

- Mantiene al usuario al margen de algunos aspectos físicos y funcionales de la red de paquetes.

- Se encarga de la facturación entre los extremos.

Nivel 5 ó de Sesión.

- Interfase del usuario con el nivel de transporte.

- Ofrece un mecanismo organizado de intercambio de datos entre usuarios.

- Trata directamente el problema del acceso de terminal remota.

- El usuario puede seleccionar el tipo de control y sincronización que desee de la red.

- Posee una serie de servicios específicos, primitivas y unidades del protocolo de datos, definidas en documentos de ISO y CCITT.

Nivel 6 ó de Presentación.

- Asigna una sintaxis de datos, esto es, determina la forma de presentación de los datos según este modelo sin considerar significado o semántica.

- Acepta tipos de datos procedentes del nivel de aplicación y negocia con el nivel homólogo del otro extremo la sintaxis escogida.

- Consta de tablas sintácticas.

- Puede crear visualizaciones de terminales virtuales.

- Puede resolver la recepción de un mensaje electrónico procedente del nivel de aplicación y encarga al nivel de otro extremo que proporcione al otro nivel de aplicación un formato de página determinado.

- Puede comprimir un texto o convertir imágenes gráficas en flujo de bits para su transmisión a través de la red.

Nivel 7 ó de Aplicación.

- Incluye los programas de aplicación que usa la red.

- Atiende el proceso de aplicación del usuario final considerando la semántica de los datos.

- Contiene varios elementos de servicio capaces de gestionar procesos de aplicación.

- Maneja los conceptos de terminal virtual y fichero virtual.

OSI ahora comprende cientos de estándares, cada uno de los cuales han tomado varios años en desarrollarse, conforme a lo establecido por ISO.

El mejor aspecto conocido de OSI sigue siendo el modelo de referencia OSI y sus siete capas, el cual es en sí una ayuda que permite a los desarrolladores de sistemas producir estándares de comunicaciones detallados dentro de una estructura arquitectónica consistente.

I.4.2. ANALOGÍA ENTRE EL MODELO OSI Y TCP/IP.

El modelo definido para el conjunto de protocolos TCP/IP es más simple que el de OSI. Como ya se mencionó, el modelo OSI define en forma general cómo deben de funcionar las redes. De hecho las redes que no siguen la arquitectura OSI no solo no cumplen con el modelo de las 7 capas, sino que por lo general muchas de sus capas no realizan las funciones establecidas en este modelo.

I.5. MODELO TCP/IP.

El modelo de capas TCP/IP no ha crecido desde un comité de estándares, sino que se ha desarrollado desde una serie de investigaciones que han conducido a la realización de la familia de protocolos de TCP/IP. TCP/IP se organiza dentro de cuatro capas conceptuales de software que se construyen sobre una quinta capa de hardware. La Fig 1.5. muestra estas capas y la forma en que los datos pasan entre ellas.

Capa de Aplicación. En el nivel más alto, los usuarios invocan programas de aplicación que accesan a los servicios disponibles a través de una internet. Una aplicación interactúa con el protocolo del nivel de transporte para enviar o recibir datos. Cada programa de aplicación elige el estilo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continuo de bytes. El programa de aplicación pasa los datos en la forma requerida al nivel de transporte.

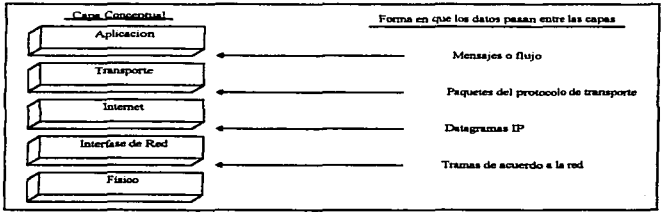

Fig. 1.5. Modelo de capas TCP/IP

Capa de Transporte. La principal función de la capa de transporte es proporcionar la comunicación desde un programa de aplicación a otro (terminal a terminal). La capa de transporte puede regular el flujo de información. Esta puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin error y en secuencia. Aunque la Fig. 1.5. utiliza un bloque sencillo para la capa de aplicación, un computador de propósito general puede tener múltiples programas de aplicación accesando a la internet al mismo tiempo. La capa de transporte debe aceptar datos desde varios programas de usuarios y enviarlos a la siguiente capa más baja.

Capa Internet. La capa Internet maneja la comunicación desde una máquina hacia otra. Esta acepta una petición para enviar un paquete desde la capa de transporte junto con una petición para enviar un paquete desde la capa de transporte junto con una identificación de la máquina a la cual el paquete deberá ser enviado. Encapsula el paquete en el datagrama IP, utiliza el algoritmo de enrutamiento y pasa al datagrama a la interfase apropiada de la red para su transmisión. También maneja la llegada de datagramas, verificando su validez, y utilizando el algoritmo de enrutamiento para decidir si el datagrama puede ser procesado localmente o se retransmite. Finalmente, la capa Internet envía los mensajes de control y errores (ICMP) tantos como sean necesarios y maneja todos los mensajes ICMP entrantes.

Capa de Interfase de Red. El nivel más bajo de software de TCP/IP comprende una capa de interfase de red, responsable de aceptar datagramas IP y transmitirlos sobre una red específica.

I.5.1. COMPARACIÓN ENTRE MODELO OSI Y TCP/IP.

Para establecer esta comparación podríamos preguntarnos: ¿Cómo está relacionado TCP/IP al modelo OSI? ó ¿Cómo se ajusta TCP/IP dentro del modelo OSI?. Para responder estas preguntas nos basaremos en la Fig. 1.6.

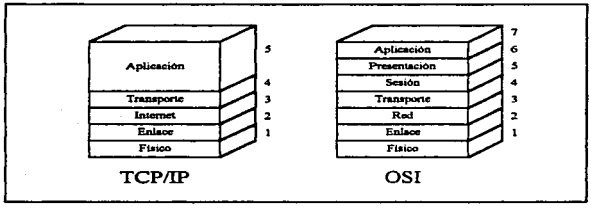

Fig. 1.6. Camparando los modelos TCP/IP y OSI

Fácilmente se observa que OSI tiene más capas que TCP/IP, pero si consideramos el funcionamiento de ambos modelos, las 4 capas inferiores son similares entre sí. Hasta la capa 2, los modelo son compatibles. OSI en las capas 1 y 2 define las normas que pueden usar los diferentes sistemas como medio de comunicación y TCP/IP no define estas capas ya que fue diseñado para ser independiente del medio, así, en principio, TCP/IP deberá correr sobre un sistema estándar OSI.

Las capas 3 y 4 de ambos modelos son comparables pero no compatibles, esto es, el modelo OSI tiene varias opciones en estas capas que se pueden usar para producir un comportamiento similar a las del modelo TCP/IP.

Las mayores diferencias ocurren en el nivel de aplicación de TCP/IP. Este nivel es separado en 3 por el modelo OSI, incluyendo el nivel de presentación. Esta es quizá la diferencia más significativa entre los 2 modelos de protocolos. El nivel de presentación de OSI trata directamente con el problema de la transportación e interpretación de la información entre computadores de arquitecturas diferentes. En OSI, el poder de estas funciones es muy superior a las del tradicional TCP/IP. Con OSI esto debería ser más fácil para lograr compatibilidad e interoperatividad entre sistemas diferentes, aunque algunos dirían que es una reducción significante en funcionalidad.

Así a la pregunta de cómo se ajusta TCP/IP al modelo OSI, la respuesta en sentido estricto es que no lo hace. TCP/IP y OSI son similares en ciertos aspectos y con propósitos similares pero ellos son claramente diferentes en la forma en que operan. A un nivel más bajo, ellos deberían coexistir, pero ellos no pueden interconectarse (sin un gateway).
A la pregunta de cómo se relaciona TCP/IP con OSI, estos empatan en los niveles 1 y 2 y tienen una igualdad razonable en los niveles 3 y 4. En los niveles más altos, TCP/IP carece de un nivel de presentación poderoso, haciendo más difícil proporcionar plena transparencia.

Otra de las diferencias importantes entre estos modelos es la forma en que se han desarrollado. Mientras que OSI comprende cientos de estándares, su proceso de desarrollo parece haber llegado a enredarse en procedimientos, los cuales caen en las dificultades de obtener consensos en grandes comités y seguido por una serie de políticas, lo que sin duda alguna han retrasado, sin intención, el proceso de desarrollo OSI y la liberación de los útiles productos que lo conforman. Por otro lado, con un punto técnico y geográfico más restringido, los desarrolladores de TCP/IP, adoptaron un enfoque más práctico. La estandarización TCP/IP fue basada en los Requerimientos para Comentarios (Request for Comments, RFC), un proceso rápido y flexible de estandarización utilizando el correo electrónico para publicar e intercambiar comentarios e ideas y así obtener una actualización fácil de los documentos.

Ni OSI ni TCP/IP se han desarrollado aisladamente. Ellos han tenido un intercambio considerable de ideas y técnicas, particularmente evidente en los cambios de OSI desde mediados de los 80's con el desarrollo de un conjunto de protocolos OSI orientados a no conexión. Los estándares OSI no han sido ignorados por los proveedores. Así con TCP/IP en los E.U.A., las universidades se han mantenido ocupadas desarrollando implementaciones OSI y los gobiernos tienen, desde mediados de los 80's, productos requeridos conforme a OSI (particularmente los gobiernos Europeos a través de las directivas de la Comisión Europea). Pero esta actividad no ha creado todavía una demanda en el mercado general ni el mismo nivel de productos de computación OSI completamente desarrollados, solo quizá con la notable exepción del equipo de red X.25.

El impacto de TCP/IP ha sido más satisfactorio y le ha asegurado un movimiento más rápido que el de OSI. Los gobiernos y las organizaciones comerciales a nivel mundial han esperado pacientemente para que OSI está disponible y poder aprovechar los beneficios de la flexibilidad prometida de un estándar internacional para comunicación e interoperación de computadoras. Basta decir que el desarrollo de OSI se ha rezagado considerablemente a lado de TCP/IP, a pesar del respaldo de numerosos gobiernos (desde 1985, el gobierno de los E.U.A. y su Departamento de Defensa).

Los administradores de los sistemas de información en compañías comerciales ahora ven a TCP/IP como una alternativa totalmente funcional, probada y de bajo costo para la interconexión de sistemas abiertos. OSI en comparación continúa siendo inmaduro y poco útil. Esto puede cambiar a mediados de los 90's, pero el interés explosivo en TCP/IP podría, por un lado retrasar la implantación de OSI y por el otro, alentarlo conforme las grandes organizaciones se tropiecen con las conocidas limitaciones fundamentales de TCP/IP.

I.6. EL PROTOCOLO TCP/IP.

TCP/IP es un conjunto de protocolos interrelacionados que permite a un proceso hablar con otro a través de una red (Internet) de una manera transparente para los usuarios.

Este diálogo entre máquinas se puede efectuar sin importar la arquitectura de las computadoras ni el tipo de red, siempre y cuando esta última cumpla con las características de Internet.

Está compuesto fundamentalmente de 2 protocolos:

- TCP resuelve el problema de transporte y siendo un protocolo orientado a conexión, realiza el control de flujo y la detección/corrección de errores, proporcionando un servicio de transporte de paquetes de información confiable entre los procesos que se comunican.

- IP se encarga del problema de ruteo (enrutamiento), proporcionando las funciones para la transferencia de la información entre dispositivos a través de una serie de redes, pero siendo un protocolo orientado a no conexión, no garantiza una entrega confiable de la información.

TCP/IP fue desarrollado para trabajar de una manera independiente del medio físico de transmisión, por lo que puede utilizarse sobre una gran variedad de redes, tales como Ethernet, Token Ring, X.25, FDDI entre otras.

Existe una serie de aplicaciones en TCP/IP que proporcionan interoperatividad entre sistemas de diferentes proveedores, utilizadas como herramientas de comunicaciones, tal como la transferencia de archivos y el correo electrónico.

Tratando de proporcionar una idea clara y general del funcionamiento de TCP/IP, en la Fig. 1.7. se muestra la manera en que los datos se envían entre dos computadores.

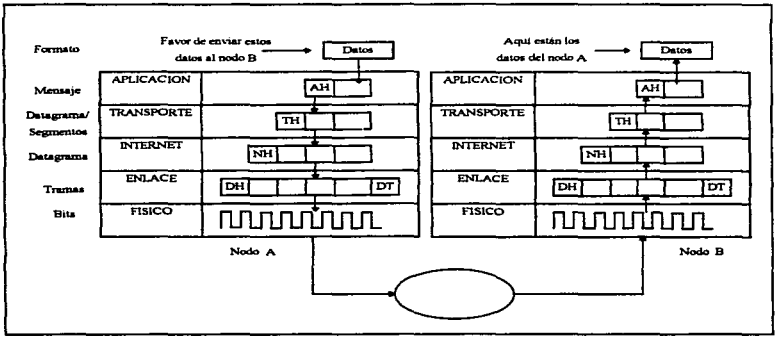

Fig. 1.7. Funcionamiento de TCP/IP.

Los encabezados que se añaden en cada capa del protocolo son mensajes entre las capas equivalentes en las dos máquinas. Se puede considerar como que cada capa envía información directamente a su compañero (capa equivalente en el otro extremo) con instrucciones relacionadas a la información transportada. a

las capas no les importa como la información fue transportada, solamente que esté correcta y qué hacer con ella. La información del encabezado permite asegurar que los datos alcancen el computador correcto y la aplicación requerida en ese computador.

II. DIRECCIONAMIENTO.

II.1. IDENTIFICADORES UNIVERSALES.

Un sistema de comunicación se dice que soporta un servicio de comunicación universal si éste permite que cualquier host se comunique con cualquier otro host. Para hacer nuestro sistema de comunicación universal, necesitamos establecer un método globalmente aceptado de identificación de computadoras o host que se unen a éste.

A menudo, los identificadores para un host son clasificados como *nombres*, *direcciones* o *rutas*. Un nombre indica cuál es el host, una dirección identifica en dónde está y una ruta nos dice cómo llegar a él.

Aunque estas definiciones son intuitivas, pueden ser engañosas. Nombres, direcciones y rutas representan sucesivamente los niveles más bajos como identificadores de un host. En general, los usuarios prefieren pronunciar nombres para identificar máquinas, mientras que el software trabaja mucho mejor con una representación más compacta de los identificadores que si pensamos en direcciones. Ambos podrían ser elegidos como identificadores universales TCP/IP.

II.1.1. DIRECCIONAMIENTO IP.

La dirección IP es un componente del Protocolo Internet. La dirección IP es un número único que identifica la conexión de una computadora o *host* (o sistema final como lo llamaría OSI) a una red física, y con la cual éstos se comunican con otras computadoras (o sistemas finales). *Host* con más de una conexión tienen una diferente dirección IP para cada una. Los ruteadores IP también tienen sus propias direcciones IP por lo que ellos pueden ser fuente y destino de datagramas IP.

El propósito de la dirección IP es doble: identificar cada conexión a la red de tal forma que sea independiente del nivel físico de la red y unir un grupo de conexiones para simplificar el enrutamiento. Los ruteadores de red usan direcciones IP para tomar decisiones de enrutamiento.

II.1.2. LA NECESIDAD DE MANEJAR DIRECCIONES.

Las direcciones IP deben ser únicas en la comunicación dentro de una red, de no ser así, las comunicaciones fallarán.

Ya que los protocolos TCP/IP no proporcionan un medio técnico por el cual las direcciones IP se pueden hacer automáticamente únicas, les toca a los administradores de la red configurar y manejarlas correctamente mediante métodos manuales tradicionales apoyados por bases de datos y una tecnología de manejo de red.

II.1.3. CARACTERÍSTICAS DE LAS DIRECCIONES IP.

La dirección IP es un número de 32 bits el cual debe ser único dentro de la red. Como mencionamos anteriormente, las computadoras con más de una conexión de red tienen una dirección IP diferente para cada conexión. Dentro de la literatura de TCP/IP a tales computadoras se les llama ***multihomed***. Estas conexiones usualmente están en diferentes redes (Fig. 2.1.). Esta es la razón por la que el número de conexiones entre redes es más que la cantidad de computadoras conectadas pero a menudo estos números son muy similares.

A diferencia de algunos otros esquemas de direccionamiento de redes, la dirección IP no necesariamente expresa cualquier información sobre la ubicación geográfica.

Dada una dirección IP usted puede deducir una autoridad de manejo; esta autoridad podría manejar una red corporativa la cual en si misma tiene una cobertura global y encaja con muchas otras redes globales.

Esto tiene implicaciones interesantes para el enrutamiento entre dos redes mundiales. Por otro lado, el esquema de direccionamiento IP *no es jerárquico.*

Los administradores de redes pueden elegir e imponer una jerarquía geográfica u organizacional en direcciones IP, pero esta jerarquía no es una función de los estándares de Internet.

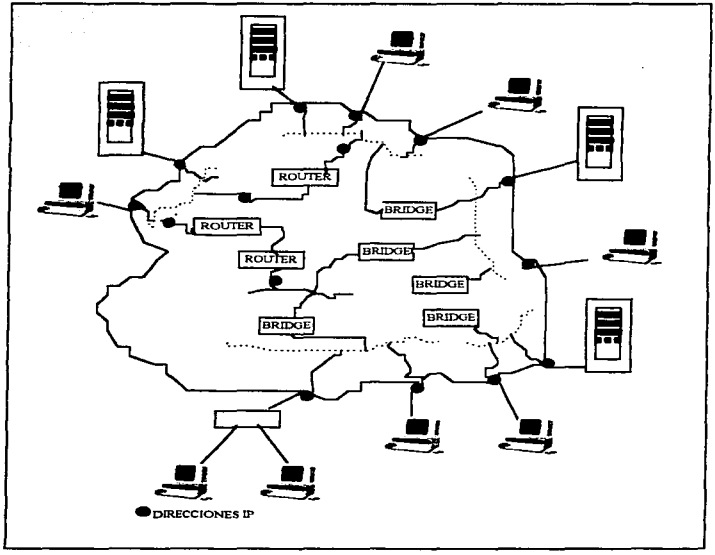

Fig. 2.1. Formato y Componentes de la dirección IP.

II.1.4. FORMATO Y COMPONENTES DE LA DIRECCIÓN IP.

La dirección IP de 32 bits tiene dos componentes (Fig. 2.2.): un **número de red** (o identificador de red) y un **número de host** (o identificador de host). Algunos "bits de clase" se pueden extraer del número de red, pero intentar examinarlos puede confundirnos. Es recomendable solo pensar que el número de red contiene los bits de clase.

El número de red identifica una organización y el número de puerto identifica una conexión particular con la autoridad de esa organización. El término "número de host" es histórico, y este nombre podría confundirnos en un *host multihomed* que tiene más de una dirección IP y por consiguiente más de un número de host. Por razones que llegarán a ser evidentes posteriormente, sería inusual que para dos puertos en la misma máquina se tenga el mismo número de red.

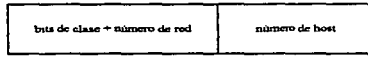

Fig. 2.2. Formato de la dirección IP.

Los términos ***net id*** y ***host id*** son comunmente utilizados para el número de red y el número de host.

II.2. CLASES DE DIRECCIONAMIENTO.

Las direcciones IP se dividen en 5 clases de dirección (**A** a **E**). Es importante entender que estas divisiones fueron concebidas para facilitar el manejo de direcciones por la IAB (Internet Activities Board).

Las primeras tres clases A, B C están disponibles para una localización normal y para comunicaciones entre dos *hosts*. Las direcciones de clase D y E no son de uso general; la clase D está reservada para sistemas *multicast* y la clase E para uso especial de la IAB.

No hay distinciones prácticas en la manera de cómo los sistemas de computadoras con direcciones de clase A, clase B o clase C usan aquellas direcciones. Con algunas excepciones, las cuales discutiremos más adelante, cualquier dirección de cualquier clase es equivalente para propósitos de comunicación. En principio, cualquier *host* se puede comunicar igualmente bien usando una dirección de cualquiera de estas tres clases. La característica que distingue a cada clase de dirección es la cantidad de números de red y el número de conexiones de host que cada número de red puede soportar. Las limitaciones de cada clase son mostradas en la Tabla 2.1.

	126	16 777 214
	16 382	65 534
	2 097 150	254
	No aplicable- reservado para sistemas multicast	
	reservado para uso del IAB	

Tabla 2.1. Limitaciones de cada clase de dirección IP.

II.2.1. NÚMEROS DE RED Y NÚMEROS DE HOST.

La opción de números de red es más importante.

Conexiones a la red con el mismo número de red se comunican directamente en esa misma red.

Conexiones a la red con diferentes números de red tienen que usar los servicios de un ruteador. Este ruteador está directamente conectado entre las dos redes a las cuales se conectan los *host* o sabe de otro ruteador el cual puede retransmitir el mensaje hacia su destino final (Fig. 2.3.).

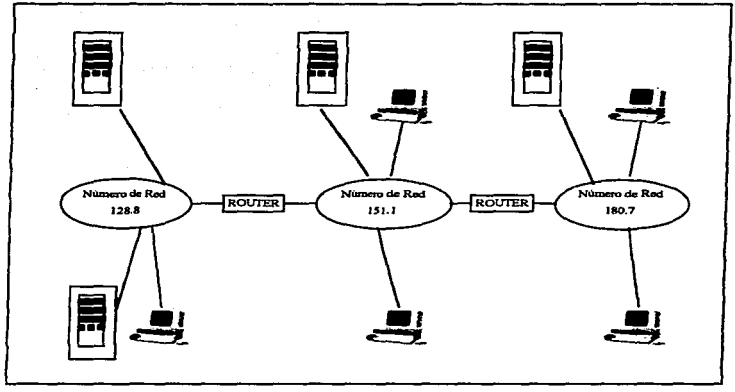

Fig. 2.3. Eligiendo números de red.

Estos factores determinan las reglas básicas para elegir los números de red y los números de hosts. Se pueden establecer alternativamente como:

Computadoras o estaciones de trabajo separadas sólo por puentes o repetidores tendrán el mismo número de red.

Computadoras o estaciones de trabajo separadas por ruteadores tienen diferentes números de red.

Para quien implanta una red, el factor más importante es que la elección de la dirección IP para un host en particular se ve afectada por la presencia de ruteadores.

El posicionamiento de ruteadores se determina por la geografía exacta de las redes físicas de capas las cuales conectan computadoras, pisos, edificios, lugares y países dentro de una interconexión completa. Esto es también fuertemente influenciado por necesidades organizacionales, flujos y volúmenes de tráfico. La configuración cambiará como se desarrolle y madure la red. Si un puente se substituye por un ruteador, el número de red sobre uno de los lados del nuevo ruteador deberá cambiar.

Al combinar las limitaciones de la Tabla 2.1., con el número máximo de conexiones de red, utilizados para comunicarse dentro de una red (u organización), se tiene una llave para determinar cuál clase de dirección deberá seleccionarse.

La convención es que la dirección se pone por escrito, o se describe para el software, en **notación punto decimal**. Cada ocho bits de la dirección (cada octeto) se convierte a un número decimal en el rango de 0 a 255 y separados por un punto (.).

Mientras que en los E.U.A. los estándares inicialmente especificaban la "notación punto decimal", algunos usuarios de computadoras están más familiarizados con la notación hexadecimal.

Las notaciones **punto hexadecimal**[1] (y Unix o estilo C hexadecimal) y **octal**[2] algunas veces son utilizadas y serán aceptadas por algunas implantaciones (aunque no por todas). Ocasionalmente es muy útil y algo extenso, representar estos número en binario. Algunas direcciones válidas se muestran en la Tabla 2.2. Los primeros ceros en cada octeto, los cuales no tienen significado, no es necesario que se incluyan. 128.1.0.9 es válido y más usual que 128.001.000.009, aunque de esta forma también es aceptable; sin embargo 128.1.9 ó 128...9 no son válidos.

44.123.110.224	2C.7B.6E.E0	0x2c7b6ee0	00101100011110110110111011100000
129.6.48.100	81.06.30.64	0x81063064	10000001000001100011000001100100
128.240.1.109	80.F0.01.6D	0x80f0016d	10000000111100000000000101101101
192.33.33.109	C0.21.21.6D	0xc021216d	11000000001000010010000101101101

Tabla 2.2. Representación de direcciones IP.

II.2.2. DISTINGUIENDO LA CLASE DE DIRECCIÓN.

Las cinco clases de dirección ya han sido mencionadas. La clase de dirección se determina por ciertos bits dentro de los primeros ocho, esto es, en el primero de los cuatro números decimales (Tabla 2.3.). La magnitud del primer número que define la clase de dirección se proporciona en la tabla.

[1] Contando en 16s, utilizando los caracteres 0 al 9 y de A hasta F.

[2] Contando en 8s, utilizando los caracteres 0 al 7.

	0	7	1	126	0 y 127 están reservados
	10	14	128.1	191.254	
	110	21	192.0.1	223.255.254	
	1110	--	224.0.0.0	239.255.255.254	No disponibles para uso gral.
	1111	--	240.0.0.0	255.255.255.254	No disponibles para uso gral.

Tabla 2.3. Distinguiendo la clase de dirección.

Existen dos características importantes de este sistema:

(1) La división entre una clase y la siguiente es siempre la frontera de un octeto. Esto se simplifica encontrando los límites entre las clases de dirección desde cada número decimal que representa un octeto.

(2) Cuando se escribe el número de red los "bits de clase" siempre se incluyen en el primer octeto para asegurar que la clase de dirección y por consiguiente el verdadero número de red no son ambiguos.

Es importante que los usuarios de TCP/IP, se familiaricen completamente con las diferentes clases de dirección y las limitaciones que tengan lugar en el desarrollo de la red. Mucha gente nueva, al principio encuentra que el objetivo de la notación punto decimal es poco excéntrica. Pero esto puede llegar a ser la

segunda naturaleza para reconocer la clase de direcciones, el número de red y la identidad del host.

Comparando con otros esquemas de direccionamiento de red, el rango de direccionamiento TCP/IP es absolutamente limitado. Actualmente el trabajo del IAB es investigar las opciones para extender el rango de dirección.

II.2.3. EL IAB Y EL REGISTRO DEL NÚMERO DE RED.

Puesto que las direcciones en una interconexión deben ser únicas, deben tener un registro con el cual se asegure que una política puede imponerse.

TCP/IP fue desarrollado para ser utilizado en la Internet de los U.S.A.. Este conjunto de redes es administrativo por diferentes autoridades, con el IAB como autoridad totalmente designada. En este ambiente de administración transferida, el número de red tiene dos funciones. Primera, ya que cada dirección IP sobre el conjunto completo de redes interconectadas debe ser única, el número de red es utilizado para identificar una autoridad de direccionamiento (frecuentemente llamado sistema autónomo) responsable de emitir una identidad de conexión única en esa parte del espacio de dirección. La segunda función es soportar el enrutamiento.

El control de IAB asegura que las direcciones IP sobre Internet sean únicas, para registrar y enviar números de redes a organizaciones que deseen estar

conectadas a Internet. Estas organizaciones no eligen su propio número[3] de red, éste se les asigna. Acuerdan emprender responsabilidades de dirección de red, cuando requieran una ubicación oficial en IAB. Entonces deben emitir las identidades de sus host hasta que tengan su propio número de red único. Si fallan al emitir números de host únicos, solo los servicios de esa organización serán afectados.

El IAB ha transferido la labor de oficina de registrar y emitir números de red IP al registro Internet, parte de la Autoridad de Números Asignados a Internet (Numbers Assigned Numbers Authority **IANA**) la cual controla los números en el protocolo TCP/IP, el cual deberá ser administrado para garantizar su correcta operación. El registro Internet es operado por el Centro de Información de la Red del Departamento de Defensa (**DDN NIC**).

Para cualquier organización comercial, solicitar al **nic** el registro de su número de red asegura que sus direcciones IP sean únicas en el mundo entero. Pero como muestra la Tabla 2.1., el espacio de dirección IP, como las direcciones clase B, está limitada con solo 16 408 redes "grandes". La clase C proporciona más de 2.1 millones de pequeñas redes. Como el interés mundial en TCP/IP ha crecido, el espacio de dirección está ya bajo presión sobre un 50 % del espacio de dirección clase B ubicado y de todo el espacio de dirección clase A emitido o reservado.

[3] Una organización aparece y requiere de muchos números de red so los ruteadores son operados correctamente. El IAB emitirá a lo cumo un poco de números de red diferentes para una organización, la cual no podrá, aparentemente satisfacer los requerimientos para un gran ruteador de red.

Hay una buena razón para ubicar una o más direcciones clase A o clase B registradas.

En el año de 1992, el número total de hosts accesible desde la Internet a través del nombre de servicio era 727 000. Como no todas las direcciones registradas están conectadas a la comunidad de la Internet, este es un número muy conservador. El crecimiento está ya sobre la porción vertical de una curva de crecimiento exponencial.

¿Cuándo podría una organización solicitar un registro de dirección IP? Por lo menos una RFC recomienda que todos los usuarios de TCP/IP se registren. Nosotros apoyamos esa política, lo siguiente proporciona una guía acerca de que organizaciones deben registrarse en orden decreciente de importancia:

Una organización conectada a Internet mundial no tiene opción: debe solicitar un registro de número de red. Esto incluye a organizaciones fuera de los Estados Unidos que tienen una relación de trabajo con el Gobierno de los Estados Unidos y desean utilizar TCP/IP para comunicaciones con el mismo gobierno. En general las organizaciones ya conocen sus responsabilidades y ya tienen un registro.

Cualquier organización que desea comunicarse con otra organización en los Estados Unidos y que está conectada a Internet necesita un registro.

Las organizaciones que tienen o adquieren subsidiarias en los Estados Unidos y las cuales se conectan a Internet podrían considerarse registradas.

Las grandes multinacionales que desean utilizar TCP/IP para comunicación mundial pero que quizá tienen control limitado o conocimiento de las actividades de compañías operadoras individuales, pueden considerarse registradas.

Para aquellas que realicen un registro existen puntos adicionales por resolver:

Las grandes organizaciones con miles de empleados en el mundo, preferían una dirección de clase B ó clase A. Todas las direcciones clase A están localizadas o reservadas; recientes ubicaciones han estado fuera de los gobiernos de los Estados Unidos. Las direcciones clase B con 65534 conexiones difícilmente llegarán a incrementarse.

Como analizamos el uso de estas direcciones IP en TCP/IP, usted podrá descubrir que el espacio de dirección se consume más rápidamente de lo que se esperaba; en redes prácticas, no es posible utilizar el espacio disponible eficientemente. Las grandes organizaciones requerirán más de una dirección clase B para satisfacer sus necesidades.

Las pequeñas organizaciones que se registren serán alentadas para utilizar una o más direcciones clase C. Desafortunadamente, las direcciones clase C no pueden tener más de 254 conexiones. Hoy en día, este número parece pequeño,

pero como la demanda de capacidad de la red por una estación de trabajo individual se incrementa con la disponibilidad general de Pcs de 32 bits operando a altas velocidades y de computadoras RISC, esta limitación puede llegar a ser menos importante.

II.2.4. VENTAJAS Y DESVENTAJAS DE LA INSCRIPCIÓN.

La ventaja clave de la inscripción es asegurarse de cómo utilizar y extender el TCP/IP para nuevas aplicaciones, las cuales pueden incluir comunicaciones con organizaciones externas, utilizando TCP/IP, su dirección y nombramiento convenidos están protegidos. Si usted no está inscrito y una dirección repentina ocurre en el futuro, entonces la responsabilidad deberá estar sobre la organización no inscrita para realizar los cambios.

Para algunas organizaciones hay una desventaja si usted se conecta a Internet, el uso de una dirección registrada es grabada en los RFC de Números Asignados junto con un nombre de contacto el cual puede estar aproximado a la información de la red. En una aplicación de registro, el NIC requiere los detalles de dos contactos, uno administrativo y de información política y el otro, un contacto técnico para resolver problemas técnicos asociados con la red.

El RFC de Números Asignados del NIC, el cual es emitido regularmente, también graba el identificador de la red. El NIC guarda los archivos de la organización responsable así como su nombre y dirección.

II.3. DIRECCIÓN ESPECIFICA DE LA RED.

II.3.1. EL SISTEMA NOMBRE DE DOMINIO.

Tan importante es el control central de nombres en un servicio general de computación que el IAB ha producido un estándar para el sistema nombre de dominio, **DNS**. Un nombre de dominio permite a una computadora que está registrada en Internet ser identificada solamente por su nombre, en cualquier lugar del mundo. La segunda función principal del sistema nombre de dominio es traducir los nombres en la única dirección IP que le corresponde, ya que todas las comunicaciones TCP/IP dependen del conocimiento de la dirección IP. La traducción inversa también es posible.

Mientras que estas son las funciones principales del DNS, éste tiene un uso más general. El estándar permite al DNS identificar los tipos de aplicaciones que están disponibles en una máquina en particular (buen conocimiento de servicios), para identificar los gateways hacia las redes y mostrar que máquinas son capaces de retransmitir un correo y hacia qué red. Estas son algunas de las funciones requeridas por más de un directorio general de servicio.

Para trabajar con nombres, se ha definido una estructura general. Cualquier sistema en donde la responsabilidad se transfiere sucesivamente a los niveles más bajos de la estructura es "jerárquico". El sistema de nombre de dominio es jerárquico y utiliza componentes separados en un nombre completo para identificar los diferentes niveles de una dirección. Como otros sistemas

jerárquicos, éste puede ser dibujado como un árbol invertido, con el tronco (o raíz como es más a menudo llamado) identificando el nivel superior de la dirección, y entonces extendiéndose sobre las ramas, ramitas y hojas que apuntan finalmente hacia una computadora individual por nombre (ver Fig. 2.4.).

La estructura actual y aceptada de nombres de dominio se basa en la primera producida por la comunidad Internet. El sistema es un esquema flexible y comprensivo que permite utilizar dos estructuras básicas; una es organizacional, la otra geográfica. Muchas organizaciones en los E.U.A. prefieren utilizar la propuesta organizacional y no la geográfica, mientras que el resto del mundo tiende a combinar ambas estructuras.

Bajo la raíz están siete referencias de alto nivel que son organizacionales, como se muestra en la Fig. 2.5. La propuesta geográfica utiliza códigos de país. Originalmente, los países utilizarían su código de marcación internacional como una identificación, pero esto no ha ocurrido. En vez de esto, se utilizó una abreviatura de dos letras del nombre del país, como se define en la recomendación ISO 3166. Algunas de ellas se enlistan en la Fig. 2.6. Muchas conexiones no de los E.U. A. a Internet han adoptado una segunda fila de dominios que conjuntamente enlaza la clasificación de la organización utilizada en el nivel superior de Internet.

Nótese que hay un dominio de nivel superior para organizaciones internacionales (INT) que no cae dentro de otras clasificaciones.

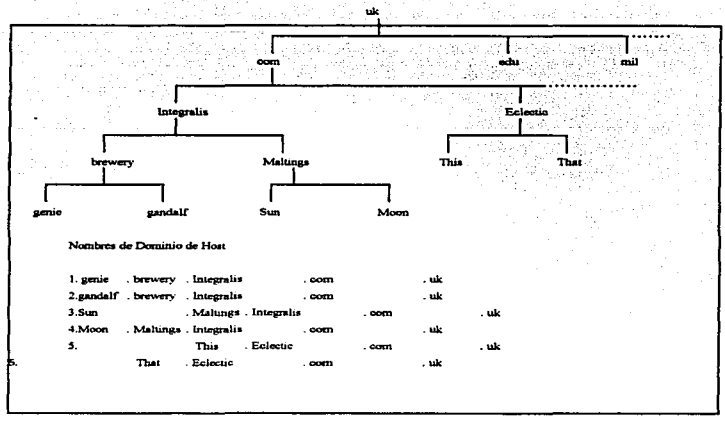

Fig. 2.4. Estructura Nombre de dominio.

II.3.2. ELIGIENDO UN ESQUEMA NOMBRE DE DOMINIO.

Una compañía grande que no desea conectarse a Internet[4] puede diseñar su propia estructura de nombramiento para enlazar a su organización. No necesita seguir estos convenios de Internet. La tecnología del DNS es independiente de

[4] Se recomienda que la emisión en cuanto a si una red se conectará o no a Internet se considere cuidadosamente antes que el direccionamiento y los esquemas de nombramiento sean puestos en vigor. Cambiarlos en una fecha posterior puede ser muy costoso.

los nombres actuales en cada nivel, se define como una extensa jerarquía consistente. Existe el dilema usual de que si el sistema de nombre de dominio podría ser puramente geográfico o puramente organizacional. Desde que el esquema de direccionamiento IP tiene una tendencia de llegar a ser geográfico para un enrutamiento eficiente, haciendo al DNS puramente organizacional podría proporcional flexibilidad adicional. Es importante que el esquema iguale a la organización lo más aproximado que se pueda, así los nombres son fácilmente reconocibles; si las etiquetas o abreviaciones existentes para las divisiones y organizaciones son adoptadas, los empleados ya estarán familiarizados con ellos.

[illegible]	[illegible]
[illegible]	Organizaciones comerciales
[illegible]	Organizaciones educacionales
[illegible]	Organizaciones gubernamentales
[illegible]	Grupos militares
[illegible]	Centros de soporte de red principal
[illegible]	Otras organizaciones
[illegible]	Organizaciones internacionales
[illegible]	Organizaciones no de los E.U.A.

Fig. 2.5. Referencias de dominio de alto nivel en Internet.

Cuando se pone por escrito, un nombre de host o un nombre de dominio completamente calificados, consiste del nombre del host o nombre del nodo seguido por todos los componentes del dominio en orden ascendente de autoridad como se muestra en el ejemplo de abajo. El nombre termina con la

raíz del sistema. Cada componente es separado por puntos. Un esquema de direccionamiento diseñado para una compañía internacional podría ser:

nodo.sitio.departamento.división.compañía.organización.país

por ejemplo:

gandalf.theale.development.integralis.co.uk

El cual se traduce para la máquina llamada Gandalf en Theale de la división de desarrollo de la compañía Integralis la cual es una compañía comercial co[5] en el Reino Unido (U.K.).

[5] Para algunos países, incluyendo al Reino Unido UK, la abreviación 'co' es utilizada como comercial y 'ac' es utilizada para la comunidad académica más bien que los equivalentes US de 'com' y 'edu'. La definición de nombres de dominio es más confusa por la existencia de un esquema anterior de la UK joint Academic NETwork (JANET), donde el componente más significativo está a la izquierda -uk.ac.umist.cs.

[illegible]	[illegible]	[illegible]
	Australia	Algunas veces OZ AU ó OZ
	Bélgica	
	Canada	Algunos sistemas Canadienses usan convenios de los Estados Unidos
	Suiza	
	Alemania	
	Dinamarca	
	España	
	Finlandia	
	Francia	
	Grecia	
	Italia	
	Japón	
	Kuwait	
	Holanda	
	Noruega	
	Nueva Zelanda	
	Suecia	
	Estados Unidos de América	Una segunda fue definida para especificar el Estado en donde estaba el host, por ejemplo, CA.US para un host en California

II.4. SISTEMA AUTÓNOMO.

Un sistema Autónomo (AS) es un conjunto de redes y ruteadores interconectados que están bajo control de una autoridad de dirección responsable de su configuración, direccionamiento, nombramiento y decisiones de enrutamiento. Las decisiones tomadas por una autoridad no pueden ser visibles para el resto de Internet. Idealmente, una organización comercial puede

formar un sistema autónomo. El IAB también registra números de AS como única identificación de un sistema autónomo.

El concepto de Sistema Autónomo se extiende en Internet a la Confederación Autónoma, un grupo de sistemas autónomos con un interés común que requieren establecer enlaces directos entre unos y otros antes que enrutarse a través de Internet.

El término Confederación autónoma es de menor importancia para las organizaciones comerciales, a menos que no lleven a cabo una sencilla autoridad de control centralizada. Este término parece que está cayendo en desuso con los cambios en la política de Internet.

II.4.1. NÚMEROS DEL SISTEMA AUTÓNOMO.

Así como la inscripción de un número de red, las organizaciones comerciales ahora pueden inscribir un número AS. El número AS es utilizado por ruteadores con los recientes protocolos de enrutamiento OSPF y BGP para identificar cuál es la fuente de información de enrutamiento. Esto forma parte de una facilidad de bajo nivelo de seguridad.

Algunas organizaciones tienen registrados más de un número AS. Los números AS solo pueden distinguir 65 535 organizaciones diferentes, así que con el curso debido, esto podría llegar ser otro escaso recurso, con el rápido crecimiento en el interés de interconectarse con TCP/IP.

Puede haber ventajas dirigidas en una gran organización utilizando varios números AS para identificar la autoridad responsable de la configuración de un dispositivo particular. Esta información normalmente se puede derivar del número de red.

II.4.2. CÓMO ELEGIR SU PROPIO NÚMERO DE RED.

La recomendación inmediata es no lo haga. Solicite un registro de dirección, pero si decide que la inscripción es innecesaria, entonces considere cuidadosamente cuál dirección elegir.

El tamaño máximo probable de red es el factor más importante que influirá en la elección de una clase de dirección IP. Las redes autónomas privadas pueden utilizar uno o varios diferentes números de red, aunque existen buenas razones para limitar el rango de números de red utilizados.

Es importante guardar como únicas las direcciones IP en cualquier interconexión de máquinas con intercomunicación TCP/IP. Así como las redes crecen y se desarrollan y como TCP/IP se utiliza para comunicar con otras compañías externas (por ejemplo Electronic Data Interchange, EDI), este llegaría a ser más difícil si el número de red no se registra y una gran cantidad de números de red está en uso. Una dirección es más probable que sea única si el número de red se registra. Si su organización no cae dentro de este grupo, el cual puede ser registrado, entonces reduce la posibilidad de una duplicidad en la dirección con otra organización y en el futuro podrá:

- Evitar direcciones de clase A, para ellas están todas asignadas a las redes más grandes a las cuales cualquiera se conecta.

- No copiar ejemplos proporcionados en los manuales de los fabricantes, libros de texto o literatura en venta.

- Evita el mejor conocimiento de direcciones publicadas en las recomendaciones (RFC's) de TCP/IP y otra documentación.

- Utilizar uno o un número limitado de direcciones clase B al azar en la mayor parte del rango de direcciones que pueden ser ubicadas hoy en día.

- Utilizar un número limitado de direcciones de clase C elegidas en forma similar.

Si en algún punto se desea emprender comunicaciones limitadas con un pequeño número de organizaciones en los direccionamientos son incompatibles, entonces no todo está perdido. Un ruteador que realiza la traducción de una dirección entre dos redes puede proyectar un limitado número de direcciones no utilizadas desde una red hacia la otra. Pero el ruteador debe aislar efectivamente el espacio de dirección de los dos sistemas.

II.4.3. DIRECCIONES IP RESERVADAS.

Ciertamente los números de redes y números de host están reservados para el uso de aspectos particulares de comunicación TCP/IP. No todos estos protocolos son utilizados con regularidad. Si usted configura una conexión con una dirección IP reservada, las fallas provocadas es probable que sean obscuras, aparentemente intermitentes y difíciles de aislar. No todos los host verifican (o no son capaces de verificar bajo todas las circunstancias) que la dirección IP solicitada para ser utilizada sea inválida.

Las siguientes direcciones están reservadas:

- Número de red 127.X.X.X, donde X.X. X. es cualquier conjunto de números. Este es utilizado para una prueba de software local loopback[6].

- Un número de red de 0's es de menor clase y significa "mi red actual en la cual no conozco el número de", algunas veces se refiere a "esta red".

- Un número de red de 1's.

[6] Los estándares IAB mencionan que cualquier dirección que comience con 127. no debe ser transmitida a través de la interfase física y aparecer sobre el cable. No todas las implantaciones de software verifican y rechazan las direcciones IP que comienzan con 127 y algunas transmitirán datagramas IP con esa dirección fuente o destino.
Esto se conoce como una causa de falla en las redes.

- Número de Host 0 es reservado para referirse a un número de red particular. Por ejemplo, 192.0.0.1. es la primera dirección de clase C que podría ser ubicada.

- Número de Host "todos 1's" es reservado para transmitir a todos los Hosts sobre una red especifica; esta puede ser utilizada solamente como una dirección de destino.

- La dirección completa 0.0.0.0. es reservada. Se utiliza en dos formas: como una dirección fuente cuando el Host no conoce su dirección genuina y por ruteadores en una lista de direcciones para anunciar la ruta por omisión, la ruta para todas las redes que no son listadas explícitamente. (Esta no es una dirección fuente o destino, meramente es una entrada en la jaula).

- La dirección completa 255.255.255.255 esta reservada como dirección de destino que significa "transmitir a todas las host sobre mired", 0.0.0.0. como un destino es una forma obsoleta de 255.255.255.255.

Más direcciones llegan a reservarse cuando se introduce una sub-red. Estas son más difíciles de reconocer.

II.5. ACCESO A INTERNET EN MÉXICO.

Actualmente existen en México algunas empresas que proporcionan todas las facilidades para conectarse a Internet a través de un módem, software de comunicaciones, y una computadora personal. Estas empresas son: SPIN, Compuserve, MS Network, Internet de México, entre otras. Los costos son de aproximadamente 15 dólares mensuales por dos horas diarias.

Para empresas grandes o escuelas, es posible accesar directamente por el Tecnológico de Monterrey utilizando enlaces **e1** y ruteadores con costos del orden de 10,000 dólares por equipo más 500 dólares mensuales, además de la renta de los enlaces **e1**.

III. PROTOCOLOS DE TRANSPORTE.

El protocolo Internet (IP) ocupa el nivel más bajo de la pila de protocolos de TCP/IP. IP es la capa 3 o componente de red del modelo TCP/IP, y proporciona las funciones necesarias para la transferencia de información entre dispositivos a través de redes estratificadas. Las funciones básicas proporcionadas en la capa de red están relacionadas directamente con el transporte de datos a la máquina correcta sobre una red física; dicho de otra forma, el enrutamiento se efectúa en esta capa.

IP se describe como un servicio de datagramas orientado a no conexión. Los datagramas son paquetes de información que pueden ser enviados a una, varias o todas las estaciones; ellos pueden tener una o varias direcciones de destino dependiendo de la cantidad de receptores a los que son enviados. No es un requerimiento para el receptor o receptores enviar al transmisor un reconocimiento de que el datagrama fue recibido. La corrección de errores no toma lugar en este nivel y la confiabilidad del servicio depende solamente del funcionamiento básico de corrección de errores que se realiza en las capas inferiores. El servicio es orientado a no-conexión (o sin conexión), porque no hay un establecimiento de llamada o circuito virtual antes de que la transmisión de datos comience; cada datagrama contiene toda la información necesaria para enrutarse correctamente.

En un servicio de datagrama son conexión, cada datagrama es considerado como completo. No existe el concepto de secuencia de datagramas preparando

un mensaje. El servicio de datagrama no tiene que recibir los datagramas en el mismo orden en que fueron enviados. Si es importante, una estación receptora debe permitir que la información que la información llegue en desorden así como recibir datagramas duplicados ya que por alguna razón fueron retransmitidos por la estación emisora.

Como IP es orientado a no conexión, los datagramas pueden viajar por diferentes rutas y alcanzar su destino posiblemente en un orden diferente al que fueron enviados. Esto es muy flexible porque los datagramas no tienen que establecer una conexión fija a lo largo de una ruta y pueden fácilmente ser reenrutados con un pequeño retardo si existe alguna falla en la red.

Una de las principales funciones de la capa IP es hacer que los protocolos de los niveles altos, ignoren cualquier cosa acerca de las características físicas del medio de transmisión que los soporta. IP proporciona una barrera entre los niveles físicos y la siguiente capa, el protocolo de transporte. Esto es importante para los desarrolladores de aplicaciones, ya no necesitan conocer los distintos medios de transmisión de los diferentes proveedores.

III.1. LAS FACILIDADES DE IP.

Para los datagramas, las facilidades básicas de IP están relacionadas con el direccionamiento, la fragmentación y la obtención de un Tipo de Servicio apropiado. Existe algunos manejadores poderosos de red y opciones disponibles de seguridad, pero se usan raramente.

El IP codifica el número de red como parte de la dirección IP; algunos protocolos (XNS, IPX) tienen un campo completamente separado para un número de red que ellos llaman la dirección de red. El número de red en el direccionamiento IP es utilizado para determinar como enrutar el datagrama.

La dirección IP únicamente identifica una conexión individual sobre un número de red particular en un camino estándar el cual es completamente independiente de la tecnología de red de esa conexión. La dirección del nivel de enlace podría ser la dirección MAC de una tarjeta LAN o de una dirección X.121 en una red X.25.

Frecuentemente se muestra dentro de la capa (Fig.3.1.) que existen otros tres protocolos que son necesarios para algunos tipos de medios físicos. Ellos son:

1.) Protocolo de Resolución de Dirección.
(Adress Resolution Protocol, ARP)

2.) Protocolo de Resolución de Dirección Inverso.
(Reverse Address Resolution Protocol, RARP)

3.) Protocolo de Mensajes de Control Internet
(Internet Control Message Protocol, ICMP)

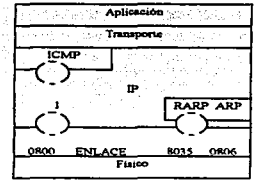

Fig. 3.1.- La Arquitectura IP.

Todos ellos serán cubiertos en detalle más adelante. ARP y RARP se muestran en la parte baja de la capa IP porque no utilizan IP y son reconocidos como protocolos separados por la capa de enlace que los soporta. ICMP ase muestra en la parte superior de la capa IP y es transportado a través de la red en datagramas IP.

III.1.1. ENCAPSULAMIENTO.

Tanto el encabezado como el campo de datos del datagrama IP llegan a ser el campo de datos de la trama generada por la capa de enlace. Esto es llamado encapsulamiento o, algunas veces envolvimiento. El campo de datos del datagrama IP contiene encabezados de los protocolos de más alto nivel y a final de cuentas la información del usuario final; IP por sí mismo encapsula los protocolos de los niveles más altos. Un ejemplo se muestra en la Fig. 3.2. Esta muestra como IP es encapsulado en las tramas de Ethernet e IEEE802.3.

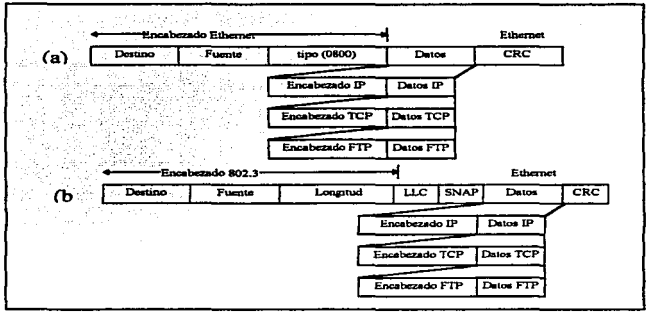

Fig. 3.2.- IP en (a) red ethernet y (b) tramas 802.3

III.1.2. FRAGMENTACIÓN, REENSAMBLE Y LA UNIDAD DE TRANSFERENCIA MÁXIMA.

Una de las funciones de IP entre la capa física y la capa de transporte es encubrir la cantidad limitada de datos que puede ser enviada en las tramas de la capa de enlace. La capa IP tiene que dar la impresión de no tener restricción en la cantidad de datos que pueden ser transmitidos a la vez. En principio los protocolos de las capas altas pueden enviar un datagrama de cualquier tamaño. IP tiene que dividir los datagramas que son demasiado largos para poder ser manejados por el medio físico, fragmentándolos para poder transmitirlos y reensamblandólos en el extremo remoto para presentarlos como si fueran datagramas sencillos. El proceso es llamado fragmentación y reensamble. Por

ejemplo, IEEE 802.3 y los sistemas Ethernet tienen un tamaño de datos máximo de 1,492 y 1,500 octetos respectivamente. El límite para las tramas IEEE 802.5 no está definido, pero en la práctica no se utilizan más de 8,192 octetos . Los paquetes utilizados en un sistema X.25 son a menudo no mayores a 128 octetos.

Este tamaño límite visto por IP es conocido como la Unidad de Transferencia Máxima (MTU). En algunas, pero no todas las implantaciones TCP/IP, este valor puede ser ajustado para cada interfase. Normalmente no es necesario hacerlo, a menos que se enlacen diferentes tecnologías LAN (anillo y bus). Para los protocolos de las capas altas, esta limitación de tamaño es invisible, asi IP tomará los datos y los fragmentará en datagramas pequeños tanto como sea necesario.

III.2. DIRECCIONAMIENTO IP.

El propósito fundamental de la dirección IP es proporcionar un esquema de dirección que sea completamente independiente del tipo de red física. La misma estructura de direccionamiento es utilizada independientemente de cualquier medio, hardware y software utilizados por las capas 1 y 2. Así desde una perspectiva de usuario o de programador de aplicaciones el esquema de direccionamiento es siempre el mismo.

Como son los sistemas telefónicos, aún cuando algunos de ellos son electrónicos y otros son electromecánicos son diseños completamente diferentes, el esquema de direccionamiento, o sea el número telefónico,

continúa siendo el mismo. Nosotros como usuarios, no requerimos conocer que el destino está en un sistema de tipo diferente; no es necesario tener diferentes procedimientos para cada sistema. Porque el esquema de direccionamiento permanece consistente y es parte de un estándar internacional, el tipo de sistema es transparente para los usuarios y para los desarrolladores de aplicaciones.

Normalmente, una dirección IP es referida a una conexión de red cuando el software TCP/IP es instalado. La dirección es configurada para representar un número de red en particular y una conexión única a un host sobre esa red. Si es hecha más de una conexión a una computadora, se requiere una dirección IP diferente para cada una de ellas.

III.2.1. TIPO DE SERVICIO.

En un intento de proporcionar un mejor servicio el encabezado IP tiene algunas banderas, los bits de Tipo de Servicio (TOS), que permiten al software solicitar diferentes tipos de funcionamiento para un datagrama: bajo retardo, alta capacidad con alta confiabilidad y bajo costo (Fig. 3.3.). En este contexto, la alta confiabilidad significa que debe haber una muy baja probabilidad de que los datagramas sean descartados por alguna congestión o error de transmisión.

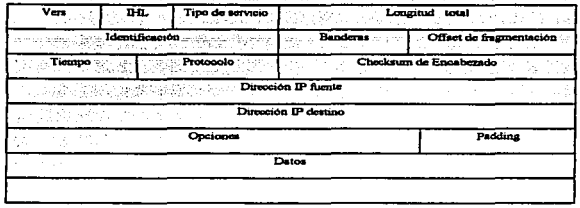

Fig.3.3. Formato del datagrama IP.

Cuando un protocolo de las capas altas solicita un TOS particular desde IP, las banderas relevantes se establecen en los encabezados IP de los datagramas; los ruteadores (o enrutadores) que procesan estos datagramas, esperan para atenderlos y proporcionarles trayectorias a través de la red que satisfagan las opciones solicitadas.

Seria poco usual que las tres opciones sean válidas y requeridas a la vez. Sus características tienden a ser mutuamente exclusivas. Es normal establecer solo uno de estos bits. Los protocolos que soportan un tráfico interactivo necesitan un bajo retardo, ya que el funcionamiento requerido por los usuarios es afectado directamente por largos retardos.

Las grandes transferencias de datos que involucran grandes bloques de información requieren canales de alta capacidad. Los protocolos de las capas superiores que proporcionan servicios de datagrama deberán requerir una alta confiabilidad. Para aplicaciones TCP/IP estándar, los TOS recomendados para

Telnet es el bajo retardo; para FTP es de bajo retardo para la conexión de control y alta capacidad para las conexiones de datos.

Un usuario o administrador de la red normalmente no tiene acceso a los valores de TOS; ellos son predefinidos por los desarrolladores cuando realizan el software de TCP/IP.

Conforme las implantaciones mas flexibles de TCP/IP llegan a estar disponibles, es conveniente revisarlas para ver que productos soportan los TOS, si esto se ve como importante para la funcionalidad del sistema. Recordar sin embargo, que solo los ruteadores pueden tomar decisiones sobre estos bits de servicio. TOS solo es importante en las interconexiones que contienen ruteadores y solo si éstos soportan el enrutamiento TOS. Algunas herramientas de diagnóstico utilizan a los TOS con propósitos de prueba, por ejemplo, verificando qué hacen con ellos los ruteadores.

III.2.2. EL DATAGRAMA IP.

El datagrama IP mostrado en la Fig. 3.3. y como establece el estándar para los sistemas TCP/IP, se presenta con una extensión de 32 bits. El orden para su transmisión es de la parte superior izquierda a la inferior derecha. Este orden de transmisión es llamado **orden de byte de red** y se aplica a todos los diagramas relacionados con TCP/IP. Así como los números son representados con los componentes más significativos a la izquierda, todos los números TCP/IP son transmitidos por el primer octeto más significante.

Ahora se describirán los campos del encabezado en orden:

Versión - 4 bits. Este campo indica la versión del protocolo IP.

Longitud del encabezado Internet - 4 bits. Este campo indica la longitud del encabezado en palabras de 32 bits, asi, el comienzo de datos puede encontrarse fácilmente si alguna opción está presente. Este es normalmente 5, el cual indica que no hay opciones utilizadas.

Tipo de servicio - 8 bits. Este campo contiene las banderas utilizadas por los TOS y su precedencia. Los primeros tres bits son utilizados para indicar uno de ocho niveles de precedencia. Esta permite a un nodo IP designar a ciertos datagramas tener una mayor prioridad que otros. Algunos ruteadores ignoran estas banderas.

La bandera D, solicita una conexión con bajo retardo. Si existe una trayectoria hacia una red en la que un ruteador 'conozca' que hay un menor retardo que en otra, ésta será seleccionada. El tráfico interactivo usando eco remoto, podría requerir este servicio.

El bit T, significa que existe un requerimiento de alta capacidad. Una vez más, el ruteador debe intentar proporcionar una ruta para este servicio.

El bit R, solicita alta confiabilidad, indicando que haya una probabilidad mínima de que sea descartado el datagrama.

Un reciente RFC añade el bit-C, el cual solicita una ruta de bajo costo.

El último bit no es utilizado.

Longitud total - 16 bits. La longitud total del datagrama IP medido en octetos incluyendo el encabezado y los datos, El tamaño del área de los datos es calculada desde el campo de longitud total y el campo IHL.

Como este campo es de 16 bits, el tamaño máximo del datagrama será de 65535 octetos, el cual es mucho más largo que la mayoría de los soportes físicos de red. (Cuando un datagrama es fragmentado, este campo contiene el tamaño del fragmento, no el tamaño del datagrama original, así que los 16 bits son adecuados para este fin).

Identificación - 16 bits. Este es un valor entero utilizado para identificar todos los fragmentos de un datagrama. Este campo debe ser único para cada nuevo datagrama enviado por un host y es a menudo simplemente incrementado.
Es importante no pensar en estos identificadores (id) como un número de secuencia. Ya que el servicio IP es sin conexión, no hay concepto de una secuencia de datagramas y ya que el servicio IP puede soportar muchas 'conversaciones' diferentes de la capa de transporte, no hay necesariamente una correlación entre los valores de id y el orden de datagramas enviado sobre una conversación particular con otro nodo.

Este concepto será desarrollado en la siguiente sección que cubre la fragmentación.

Banderas - 3 bits. Los dos bits de más bajo orden son utilizados como banderas para controlar la fragmentación. Si el bit de más bajo orden es cero, indica el último fragmento de un datagrama y por consiguiente algunas veces es referido como la 'Bandera más' o bit MF. El bit medio es utilizado para indicar que el datagrama no puede ser fragmentado y es referido como la 'Bandera de no fragmentación' o bit DF. El bit de mayor orden no es utilizado.

Compensación de Fragmento - 13 bits. Este campo es utilizado con datagramas fragmentados para indicar la posición que el fragmento ocupa en el mensaje original. Esta compensación es medida en unidades de 8 octetos; así los fragmentos deben construirse en 8 unidades de octetos; el tamaño mínimo del fragmento es de 8 octetos de datos, no incluyendo el encabezado IP (el cual tiene 20 octetos sin opciones), ni el campo de encabezado del nivel de enlace.

Tiempo de vida - 8 bits. El campo de tiempo de vida (TTL) es definido por el emisor del datagrama y es decrementado por los ruteadores conforme el datagrama para a través de ellos. Si esta acción reduce el TTL del datagrama a cero, éste es descartado. Esto previene que algún datagrama se quede circulando indefinidamente en una red. Un ruteador nunca podrá recibir un datagrama que contenga el campo TTL puesto a cero.

El valor de TTL se puede configurar en algunas implantaciones del software TCP/IP y su valor puede ser importante. Si el valor de este campo se determina muy pequeño, es posible que los datagramas, no puedan alcanzar las partes remotas de una red muy larga; si se define muy grande, los datagramas podrían viajar innecesariamente en la red creando un tráfico poco ordinario. El valor recomendado es 32, aunque suelen encontrarse sistemas que establecen el valor máximo posible de 255 o más bajos de 3 ó 4.

Protocolo - 8 bits. Este campo indica el protocolo de la capa de transporte llevado por este datagrama. Este le dice al nivel IP qué capa de transporte pasará a este datagrama. Los valores normales para este campo son:

17	UDP
6	TCP
1	ICMP
8	EGP
89	OSPF

Checksum de encabezado - 16 bits. El checksum (Chequeo de errores) del encabezado IP es interesante porque éste solo protege el encabezado y no protege lo datos que lleva. La razón principal de esto, es que el checksum debe ser recalculado cada vez que pase a través de un ruteador, para el valor TTL, las banderas y la compensación de fragmentos pueden cambiar. Si se incluyeran los datos en el Checksum, se provocaría un retardo adicional al datagrama.

El Checksum es un cálculo sencillo. Este se basa tomando el encabezado como enteros de 16 bits, sumándolos utilizando su complemento a 1 y tomando el complemento a 1 del resultado.

Algunos sistemas que trabajan sobre detección de errores de redes no definen el checksum del encabezado.

Dirección fuente IP - 32 bits. La dirección fuente de IP.

Dirección de destino IP - 32 bits. La dirección de destino IP.

Datos - variable. Este incluye los encabezados de los protocolos de las capas altas y algunas veces datos de usuarios.

Padding (relleno) - variable. Este campo representa ceros utilizados para rellenar el encabezado a palabras de 32 bits, así que el IHL puede correctamente indicar el punto de inicio de los datos cuando las opciones de longitud variable se presentan.

Opciones. El campo de opciones soportan las facilidades de depuración, medición y seguridad. Puede haber opciones múltiples en un datagrama sencillo, cada uno con el formato mostrado en la Fig. 3.4.
En algunas implantaciones de TCP/IP la definición de estas opciones esta dentro de una utilidad llamada ping. Otras implantaciones no dan al usuario ni a la interfase de manejo de red el campo de opciones.

Los campos de opción son:

Copia (1 bit). Utilizado para indicar si esta opción será colocada en todos los fragmentos. Si esta opción tiene un cero (0). Sólo aparecerá en el primer fragmento. Las opciones de seguridad, por ejemplo necesitarán ser copiadas dentro de todos los fragmentos.

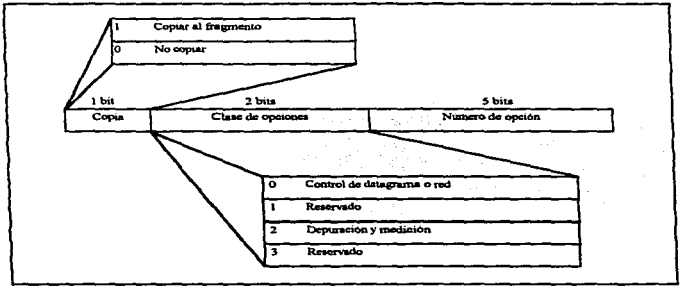

Fig. 3.4.- Opciones de medición y seguridad.

Clase de opción (2 bits). Utilizado para especificar la clase de opción. La opción para marcar tiempo tiene una clase 2, de otra manera la clase es usualmente cero (0).

Números de opción (5 bits):

Seguridad: opción 2. Las opciones de seguridad son asignadas por la Agencia de Inteligencia de la Defensa de los E.U.A. y define un datagrama desde un rango no clasificado hasta uno de alto secreto. Esto permite a un ruteador detectar los datagramas que llevan información especial y se previene para dejarlos en un ambiente seguro. Estas características no han tenido un amplio uso en las implantaciones comerciales TCP/IP.

Tiempo de sellado: opción 4. Esta opción permite a un datagrama ser enviado a través de la red y reunir marcas de tiempo por cada ruteador que pasa. Esto puede ser utilizado para evaluar retardos y sus variaciones dentro de una red de ruteadores. (Los relojes en todos los ruteadores deben estar sincronizados o usando tiempos diferenciales).

Ruta fuente libre: opción 3. Esta es otra opción de administración que permite que un datagrama sea dirigido a un grupo particular de ruteadores, utilizando una lista predefinida de direcciones IP de los ruteadores que deberán ser visitados en secuencia. Esta opción permite que otros ruteadores no incluidos en la lista se utilicen.

Registro de ruta: opción 7. Esta alternativa causa que cada ruteador coloque su dirección IP en el campo de opción del datagrama, así, este viajará a través de la red. Esta lista es utilizada para definir la trayectoria que los datagramas usarán para alcanzar un host particular o ruteador. El datagrama debe tener suficiente espacio para almacenar el número de direcciones IP que vaya encontrando.

Ruta fuente estricta: opción 9. Es similar a la ruta fuente libre, excepto que solamente los ruteadores definidos en la lista pueden ser utilizados, no otros. Si el datagrama no puede ser enrutado, resultará en un mensaje de error ICMP.

III.2.3. FRAGMENTACIÓN Y REENSAMBLE.

La fragmentación tiene un estricto significado en TCP/IP. Este es el proceso utilizado por IP para reducir el tamaño de datagramas que son muy largos para ser transportados por un medio específico. Los fragmentos no deben exceder la interfase de red MTU.

IP reduce el tamaño de un datagrama muy largo, dividiendo el campo de datos en partes pequeñas más accesibles. El encabezado IP debe ser transportado por todos los fragmentos para ser enrutado correctamente, así el tamaño del datagrama solo puede ser cambiado por reducción de la cantidad de datos.

Todos los fragmentos llevan los 32 bits del número de identificación del datagrama original. Este es utilizado para identificar los fragmentos del diagrama original cuando son reensamblados en el nodo receptor. Una vez que el datagrama ha sido fragmentado, este no será reensamblado hasta que alcance su destino final en el último nodo. Intentar reensamblar un datagrama antes de que alcance su destino podría dar lugar a dos tipos de problemas. Primero, es una red de caminos múltiples, es posible que los fragmentos tomen diferentes caminos; un nodo intermedio no los verá a todos así que no podrá reensamblar el datagrama completo. Segundo, para reensamblarlo en un nodo intermedio

(ruteador) requeriría recolectar todos los fragmentos antes de retransmitir el datagrama completo. Esto provocaría un retardo innecesario, además de que tendría que ser fragmentado nuevamente para seguir su camino.

La Fig. 3.5 presenta un ejemplo de cómo es fragmentado un datagrama. El encabezado IP se muestra al frente de los campos de identificación, las banderas y compensación de fragmentación. La figura también muestra una configuración de red que requiere una fragmentación de datagrama. La red 1 tiene un MTU de 1200, la red 2 de 532 y la red 3 de 276. (Estas cantidades son ilustrativas). Inicialmente el datagrama tiene 1024 octetos de datos cuando es transmitido a la red 1. Para el ruteador A, la capa IP que maneja la red 2, sabe que la red 2 tiene una MTU de sólo 532 y fragmenta el datagrama dentro de dos más pequeños, cada uno con 512 octetos. El encabezado IP de 20 octetos, junto con uno de los fragmentos formarán 532 octetos al nivel de la capa de enlace, la MTU para este sistema (la MTU está referida a la cantidad de datos que la capa de enlace puede llevar en una de sus tramas). La compensación del primer fragmento ser cero (0), indicando su posición en el datagrama original. La compensación en el segundo fragmento será de 512/8, ó sea 64, así, el bit 13 del campo de compensación de fragmento indica la posición en unidades de 8 octetos. El 'bit más' en el primer fragmento será 1 indicando que vienen más fragmentos; en el segundo será cero (0), ya que es el último fragmento.

Cuando los fragmentos llegan al siguiente ruteador, éstos deben ser seccionados nuevamente, identificándolos con la bandera más se pone a 1 en todos los fragmentos, excepto el último.

La compensación de fragmentación indica como deben unirse apropiadamente las piezas para formar el datagrama original.

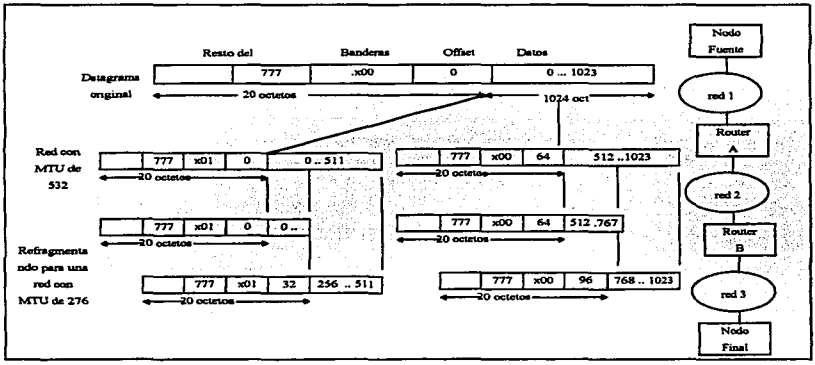

Fig. 3.5.- Fragmentación del datagrama.

Utilizando la compensación de fragmentación, el datagrama original puede ser reensamblado aunque los fragmentos lleguen fuera de orden. El nodo final inicia un temporizador que es utilizado para determinar el tiempo máximo que el nodo esperará para que todos los fragmentos lleguen, normalmente son 30 segundos. Si algún fragmento no llega dentro de este tiempo (time-out) el datagrama completo es descartado y dado que es un servicio sin conexión, IP no intenta recuperar la situación y se puede generar un mensaje de error ICMP.

III.3. PROTOCOLOS.

III.3.1. PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN.

Las tarjetas para Redes de Área Local (Local Área Network, **LAN**) envían y reciben tramas basadas en sus direcciones **MAC** (Control de Acceso al Medio / Medium Access Control). Ellas solo pueden responder a tramas que contengan en el campo de destino un broadcast (para todas las direcciones). multicast reconocido (para algunas direcciones específicas) o unicast (su propia dirección).

TCP/IP utiliza direcciones IP que son definidas por los administradores de red en el momento de instalación; ellas son asociadas con la capa de red y no tienen relación directa con la dirección MAC.

Todas las comunicaciones TCP/IP comienzan con la dirección IP. Si se desea conectar a una computadora remota se debe conocer su dirección IP sin ser necesario conocer su dirección MAC. Las comunicaciones de terminal a terminal (end-to-end) toman lugar con la dirección IP, pero las comunicaciones de salto en salto (hop to hop) usan la dirección MAC. Para una eficiente operación de red, la capa MAC requiere la dirección única de la siguiente capa MAC en la cadena de saltos entre las direcciones IP fuente y destino.

Los primeros sistemas TCP/IP debían tener una tabla configurada manualmente que relacionaba las direcciones MAC e IP, así, la trama podía ser enviada a la

destinación correcta. Actualmente, el Protocolo de Resolución de Dirección (ARP) relaciona las direcciones IP y MAC (de acuerdo al medio que las soporta).

Cada nodo mantiene un **cache** (localidad para guardar información), llamado el cache ARP, de entradas IP contra sus direcciones MAC. Cuando IP es requerido para enviar un datagrama a otra dirección IP, primero verifica en el cache ARP para encontrar la dirección MAC correspondiente que el nivel de enlace debe usar para el datagrama. Si no lo encuentra, éste intenta encontrar la dirección MAC desde la dirección IP, utilizando ARP.

Para hacer esto, ARP envía un datagrama de petición ARP a todas las tarjetas LAN, utilizando la dirección MAC para broadcast (0xFFFF_FFFF_FFFF). ARP utiliza su propio Ethernet tipo 0x0806 para estas peticiones, así que pasan por el software ARP en todos los nodos dentro del área del broadcast. El ARP solicita llevar la dirección IP correspondiente a la dirección MAC requerida. Todas las tarjetas de la red leen el datagrama de petición y si alguna descubre que coincide su dirección IP con la dirección IP solicitada contesta con una respuesta ARP. Si se recibe una respuesta, se guarda la información en el cache ARP para su uso futuro; si no hay respuesta en pocos segundos, la petición se repite (el ARP puede ser descartado por error de transmisión o congestión). Para reducir la necesidad de broadcast ARP, un nodo responde a la solicitud ARP con una copia del mapa de direcciones IP y MAC de la fuente de la petición en su propio caché ARP. Como los dos sistemas son para comunicación adicional, esto remueve la necesidad para un segundo ARP en

dirección contraria en algún tiempo posterior como si conocieran la dirección MAC para esa dirección IP de remoto.

El caché ARP normalmente se retiene hasta que el equipo es apagado o se le aplica un 'reset'. Con algunas implantaciones TCP/IP las entradas al caché ARP tienen un determinado tiempo (time.out). Si la entrada no es utilizada en cierto periodo, casi siempre 15 minutos, la entrada es borrada. Otros sistemas proporcionan un tiempo automático de borrado. Un ARP se efectúa cada 15 minutos para asegurar que el cache es actualizado. Ya que las direcciones MAC generalmente cambian cuando una pieza del equipo tiene falla o es removida, esto parece de un valor más limitado.

Algunos productos permiten ver y alternar el caché ARP y cambiar sus tiempos de control. Esta puede ser una herramienta útil de diagnóstico. Este enlista cuales hosts están comunicados con un nodo. Cuando un sistema falla y una tarjeta ha sido cambiada, el cache ARP contiene un valor desactualizado, el mapeo puede estar alterado. La traslación de dirección MAC hacia IP puede ser predefinida por hosts que no son capaces de usar ARP.

Los datagramas ARP no pasan a través de ruteadores y como un ruteador opera en la capa IP no relevará el tráfico broadcast MAC; los ruteadores crean una memoria intermedia útil entre los dominios del broadcast. Esto permite a los ruetadores prevenir el tráfico broadcast desde todas las redes en un sistema.

III.3.1.1. FORMATO ARP.

El formato del datagrama ARP se muestra en la figura 3.6. Es simple y fue desarrollado para ser genérico; no es utilizado solo por TCP/IP o por algún tipo particular de red. Existe sólo una restricción, de que el medio debe tener la capacidad para enviar tramas de broadcast.

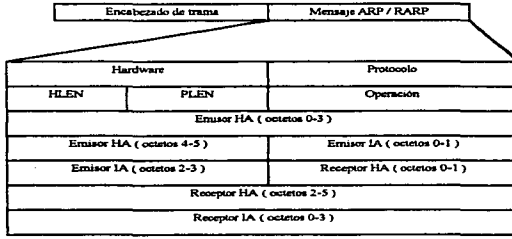

Fig. 3.6.- Formato del datagrama ARP.

ARP opera directamente sobre la capa de enlace y por tanto es encapsulado en la trama de enlace. Esto requiere tener su propio campo tipo Ethernet 0x0806 en el que la trama de enlace puede distinguirlo de entre otras tramas entrantes.

Los campos del datagrama ARP son cómo sigue:

- Hardware: Este campo indica el tipo de red (hardware) que ha generado el datagrama. Los tipos válidos son:

	Ethernet (10 Mbps)
	Ethernet experimental (3 Mbps)
	Amateur radio AX.25
	Proteon ProNET Token Ring
	Chaos
	Redes IEEE 802
	ARCNET
	Hyperchannel
	Lanstar
	Autonet short address
	LocalTalk
	LocalNet

- Protocolo: Este campo indica cuál protocolo solicita esta acción. Los valores utilizados en este campo son los mismos que el campo tipo Ethernet en las tramas ethernet. Este es 0x0800 para IP.

- HLEN: Este indica la longitud de las direcciones hardware en octetos. Tiene normalmente un valor de 6 para direcciones IEEE LAN MAC.

- PLEN: Este indica la longitud de las direcciones de capa de red en octetos y tiene normalmente un valor de 4 para IP.

- Operación: Este campo tiene un valor de 1 para una solicitud ARP o 2 para una respuesta ARP. Este campo lo utiliza RARP con valor 3 para una petición RARP y con 4 para una respuesta RARP.

- Direcciones: Dirección hardware del transmisor (dirección MAC fuente); dirección fuente IP; dirección hardware destino (dirección MAC destino); dirección IP de destino.

III.3.1.2. ARP EN OPERACIÓN.

La Fig. 3.7. muestra un ejemplo de ARP en operación. El nodo con dirección IP 128.128.0.3 y con dirección MAC 0x02608121343 ha sido solicitado por su capa IP para encontrar la dirección MAC del nodo con dirección IP 128.128.0.1. Primero, 128.128.0.3 envía una petición ARP broadcast la cual será recibida por el software ARP en todos los nodos de esa red. 128.128.0.1. reconocerá su dirección en la petición y regresará una respuesta ARP pero utilizando la dirección MAC. La respuesta ARP será procesada y rápidamente desechada por las tarjetas LAN de todos los nodos en la red como si fuera una trama unicast con la dirección de destino equivocada.

a)

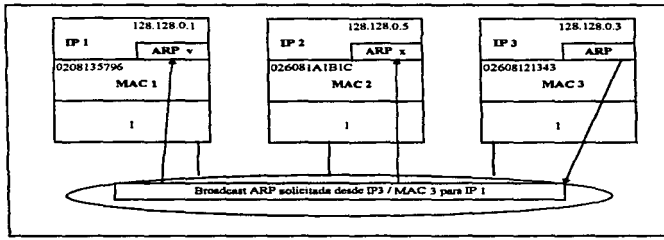

Fig. 3.7.a.- El proceso ARP.Petición ARP.

b)

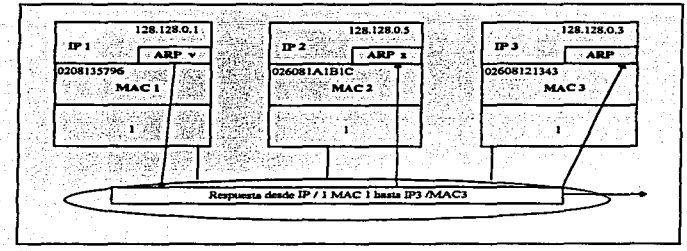

Fig. 3.7.a.- El proceso ARP.Respuesta ARP.

III.3.2. PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN INVERSO.

El Protocolo de Resolución de Dirección Inverso (RARP) está hecho para usarse con dispositivos que no pueden almacenar sus direcciones IP, normalmente estaciones de trabajo sin unidad de disco. No es de sorprender que RARP efectúe la acción inversa a ARP: dada la dirección MAC, solicita la dirección IP correspondiente. Un nodo solicitado proporciona la dirección MAC en la petición RARP.

RARP, como ARP, opera directamente sobre la capa de enlace ya que tiene asignado un número tipo Ethernet 0x8035, puede ser distinguido desde IP, ARP y algunos otros protocolos de red. Los nodos actuando como servidores RARP

que encuentran quién iguale la dirección MAC en sus tablas RARP, contestarán con la dirección IP correspondiente en una respuesta RARP. Este sistema requiere que al menos un servidor este presente y que tenga una tabla definiendo qué direcciones IP deberán ser usadas por cada dirección MAC.

El formato del datagrama es el mismo que en ARP pero en el campo de operación utiliza un valor 3 para una petición y 4 para una respuesta. Cuando se hace una petición RARP, el emisor solo conoce su propia dirección MAC así que es el único campo que puede cubrir. La respuesta normalmente tendrá todos los campos cubiertos, definiendo la dirección IP el solicitante deberá usarla y a menudo la dirección IP y MAC del servidor RARP, aunque esto no sea necesario.

Aunque RARP cumple sus intenciones originales tiene muchas limitaciones; en la práctica ya ha sido reemplazado por el Protocolo Boot (BOOTP). BOOTP es capaz de operar a través de los ruteadores y proporcionar información más útil que RARP donde las estaciones de trabajo arrancan sin disco.

III.3.3. PROTOCOLO DE MENSAJES DE CONTROL INTERNET.

Aunque IP es un servicio de datagrama no excite una garantía de que la información sea entregada. El protocolo de Mensajes de Control Internet (ICMP), se proporciona dentro de IP y genera mensajes de error para ayudar a la capa IP a proporcionar un mejor servicio. Para el manejo de red, ICMP proporciona algunos diagnósticos provechosos acerca de la operación de la red.

Las RFC para IP dicen que ICMP debe soportarse, pero el nivel de soporte varía, con frecuencia limitado para no generar un error cuando un datagrama ICMP es recibido. No todos los productos soportan a ICMP al nivel requerido de implantaciones TCP/IP sofisticadas.

ICMP utiliza datagramas para llevar sus mensajes entre nodos relevantes. Los mensajes de error ICMP son generados por un nodo reconociendo que hay un problema de transmisión, y son regresados a la dirección original del datagrama que causó el problema. La dirección original será generalmente un host o un sistema terminal. El generador del ICMP podría ser el último nodo o un ruteador intermedio. Los ruteadores y hosts pueden ser la fuente de datagramas ICMP.

La Fig. 3.8. muestra el formato básico del mensaje ICMP encapsulado en un datagrama IP y los diferentes mensajes posibles. ICMP tiene su propio número de protocolo IP (1) de tal forma que la capa IP sabe cuando son recibidos.

Aunque ICMP utiliza la capa IP es considerada por completo dentro de IP porque ésta no proporciona necesariamente un servicio en las capas superiores.

Ya que los mensajes IP son transportados en IP, ellos pueden ser descartados por las mismas razones que un datagrama IP. Los mensajes IP no son generados por mensajes IP que causen errores por sí mismos. Tampoco son generados por problemas con fragmentos IP, a menos que sea el primer uno (compensación de fragmentación = 0).

El formato básico de un datagrama ICMP se muestra en la Fig. 3.8., pero los campos varían dependiendo del tipo utilizado. El campo de tipo indica que es un mensaje relevante ICMP y el campo de código es utilizado para proporcionar información más detallada. El **checksum** (chequeo de errores), sí se usa, se requiere porque IP no protege sus datos con un checksum. Cuando opera sobre una red física la cual tiene una secuencia de chequeo de trama, el checksum del ICMP puede ser cero (0), lo que indica que no está calculado.

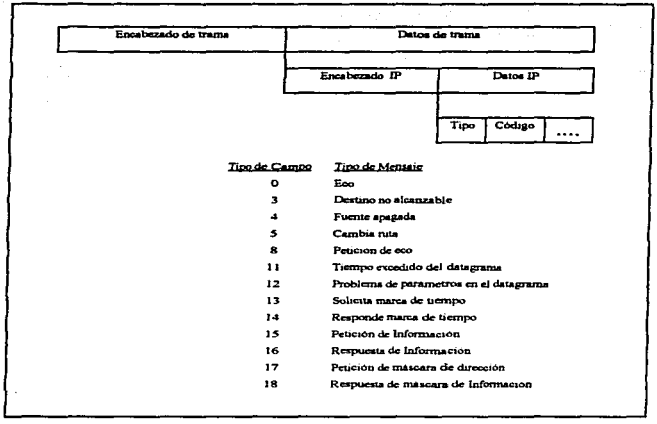

Fig. 3.8.- ICMP encapsulado en IP y sus valores tipo.

III.4. PROTOCOLOS DEL NIVEL DE TRANSPORTE.

Hasta ahora se han considerado las tramas de la capa de enlace y los datagramas de la capa IP. Los datos de IP son encapsulados por el datagrama IP el cual a su vez es encapsulado por la trama. En la capa de transporte, hay dos opciones separadas, UDP y TCP (Fig. 3.9.). Dependiendo del tipo de servicio que es requerido por la aplicación del usuario, uno de estos protocolos es llevado en el campo de datos del datagrama IP.

Una vez que la información ha sido transferida a la máquina correcta por IP, entonces, ha de ser pasada al nivel de aplicación correspondiente en esa máquina. El multiplexaje y demultiplexaje de datos de muchas aplicaciones para y desde la capa IP así como el acceso de los datos a la aplicación correcta es una de las responsabilidades de la capa de transporte. El proporcionar un servicio de flujo de datos libre de errores y de flujo controlado (orientado a conexión) o solamente pasando sobre el servicio sin conexión de IP a la aplicación correcta es también función de esta capa.

El protocolo de Datagrama de Usuario (UDP) proporciona un servicio sin conexión poco confiable. Esto permite que los datos sean transmitidos a una máquina o grupo de máquinas sin necesidad de establecer una conexión.

Los datagramas de Usuario (UDP) proporciona un servicio sin conexión poco confiable. Esto permite que los datos sean transmitidos a una máquina o grupo de máquinas sin necesidad de establecer una conexión.

Los datagramas sencillos son enviados a un nodo remoto sin algún requerimiento de respuesta que indiquen que el datagrama ha llegado.

En ciertos ambientes esta es la forma más eficiente de operar. Los servicios de Aplicación, tales como TFTP y NFS utilizan este tipo de transporte. Donde el broadcast es requerido, ésta puede ser la única opción disponible.

EL Protocolo de Control de Transmisión (TCP) proporciona un servicio orientado a conexión. Una conexión es como un "ducto" de datos que corre entre dos puntos. Con TCP no existe la facilidad broadcast o multicast. TCP tiene todas las características necesarias para proporcionar un servicio confiable entre dos computadoras. Para garantizar la seguridad, este añade una cantidad significante de encabezados que son utilizados para manejar los reconocimientos, flujo de control, temporizadores y facilidades para el manejo de una conexión.

Este tiene más encabezados que UDP, en términos de la potencia de procesamiento requerida y del tamaño de los encabezados de red que usa. Las aplicaciones que requieren este servicio son Telnet y FTP.

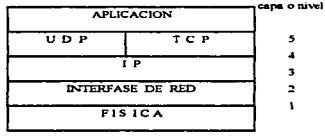

Fig. 3.9.- UDP y TCP.

III.4.1. PUERTOS.

Tanto UDP y TCP utilizan un puerto de direccionamiento para liberar la información de las capas de aplicación de servicio relevante. Un puerto tiene 16 bits de dirección de los cuales un número de puertos bien conocidos han sido

definidos dentro de un rango de 0 a 255 (Fig.3.10.). En otras palabras, los números de puerto han sido localizados por la capa de aplicación de servicios más común, tales como Telnet y FTP. Si los diseñadores de las aplicaciones crean un programa para trabajar sobre UDP o TCP, tienen que definir qué puerto desean utilizar; para asegurar esto, el número es único para cada máquina en particular ya que permite al menos tener un valor fuera del rango reservado para los puertos bien conocidos.

Existe una alternativa dinámica para esta definición de puertos. NFS utiliza un servicio conocido como mapeo de puertos, el cual permite que los puertos nuevos sean definidos y registrados dinámicamente o que el puerto utilizado para un servicio en particular sea definido sobre pedido.

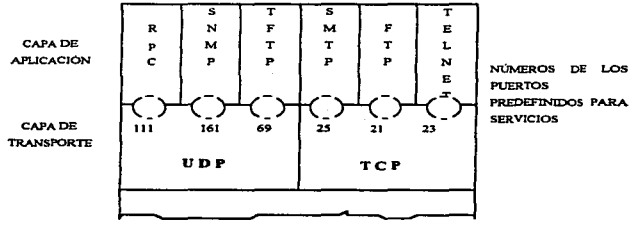

Fig. 3.10.- Puertos utilizados en UDP y TCP.

III.4.2. SOCKETS.

El término socket es frecuentemente utilizado en conjunción con TCP/IP.

Esto es solo un simple, pero muy importante concepto. El socket es un encadenamiento de la dirección IP y el número de puerto. Como la dirección IP es en principio, única de un nodo y asumiendo que todos los nodos utilizan direcciones IP registradas, y el puerto es único sobre un nodo, el socket proporciona una identificación única de un servicio de la capa de aplicación. Ya que la referencia del socket es única, tanto UDP y TCP incluyen la dirección IP y el número de puerto en su cálculo de checksum. Esto es para asegurar que los datagramas que lleguen a un host erróneo, no sean aceptados por la capa de transporte de dicho host ni por el puerto que, si es bien conocido, es probable que exista[1].

Muchas capas de servicio de aplicación permiten sesiones múltiples y entonces, necesitan estar disponibles para diferenciar estas sesiones y asegurar que los datos que se envían de regreso sean a la computadora apropiada. Por ejemplo, un número de usuarios está probablemente conectado en el mismo host utilizando Telnet (puerto 23) y muchos de ellos podrían utilizar el mismo puerto de Telnet para el acceso. Un camino para diferenciar las sesiones puede ser el

[1] Es concebible que un encabezado IP pueda tener su dirección IP corrompida y pueda llegar a la máquina errónea. Si el Checksum IP es ignorado, éste puede pasar a la capa de transporte donde el puerto será examinado.

considerar de dónde vienen los datagramas por su dirección IP, pero es posible que dos usuarios desde el mismo host puedan estar conectados a una aplicación. En este caso, podría ser extremadamente difícil separarlos.

Para resolver este problema, los números de puertos bien conocidos o predefinidos, son sólo utilizados por los servidores de la capa de aplicación de servicios. El cliente programa y selecciona un número de puerto único que no ha sido aún utilizado en la máquina. En este caso, si dos sesiones son colocadas en el mismo servidor host desde un mismo usuario, es fácil de utilizar la opción socket para ver las diferencias entre las dos sesiones, ya que ellos serán únicos.

Los servicios de aplicación transmiten de regreso la opción socket y esta es una razón del por qué tanto la dirección origen de IP y la de puerto origen son incluidas en todas las comunicaciones entre dos máquinas.

Pocos servicios que operan sobre bases de igual a igual, utilizan el mismo número de puerto para transmisión y recepción. Estas tienden a ser funciones de ruteo para transmisión y recepción. Estas tienden a ser funciones de ruteo y administración que no tienen necesidad de diferenciar los puertos cuando los mensajes regresan.

III.4.3. PROTOCOLO DE DATAGRAMA DE USUARIO (UDP).

UDP añade algo más al datagrama IP, siendo otra forma de tratar el problema de pasar datos a la capa de aplicación correcta. Esto se hace a través de los campos de origen y destino en el encabezado. El bloque de datos que pasa de UDP a IP, consiste del encabezado UDP y de los datos de la capa de aplicación, esto también es referido como un datagrama. La Fig.3.11. muestra los campos que son añadidos por UDP, estos son:

- **Puerto origen** Es el número de puerto de la capa de aplicación de servicio de donde proviene el datagrama.
- **Puerto destino** Es el número de puerto de la capa de aplicación de servicio a donde se desea enviar el datagrama.
- **Longitud** Es el tamaño del datagrama UDP
- **Checksum** Es un chequeo que se realiza para proteger los datos llevados por UDP.

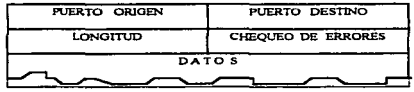

FIG. 3.11.- Campos del encabezado UDP.

El checksum es realmente básico. Se obtiene del complemento a 1 de cada palabra de 16 bits, tanto del encabezado como de los datos y el resultado se complementa a 1, tal como en IP. Lo que resulta poco usual acerca de este checksum es que no sólo considera los campos UDP, sino que también incluye lo referido a su pseudo encabezado basado en ciertos campos de la capa IP, para asegurar que el cálculo considera el socket y no sólo el puerto. (Fig.3.12.).

Algunos productos permiten configurar el tamaño máximo de un datagrama UDP. Esto sería necesario si algunos componentes del sistema no estuvieran listos para recibir datagramas grandes, pero esto es poco usual. Reduciendo el Tamaño Máximo del Datagrama (MDS) disminuye la cantidad de memoria requerida por UDP en el host, pero también reduce el desempeño de los servicios que utilizan este protocolo. Es extraño que estos valores predefinidos se requieran cambiar.

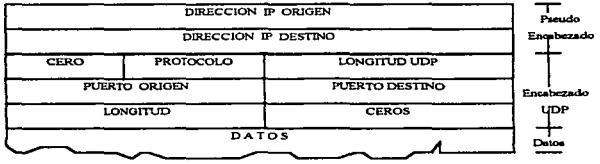

Fig. 3.12.- El chequeo de errores de UDP es en base a la información del pseudo encabezado y del encabezado.

III.4.4. PROTOCOLO DE CONTROL DE TRANSMISIÓN.

TCP añade confiabilidad a IP y como UDP, también proporciona el direccionamiento en la capa de aplicación a través del uso de puertos. TCP es un protocolo orientado a conexión; no sólo es confiable, sino que antes de que la transmisión comience desde una máquina a otra, una conexión debe abrirse. Cuando la transmisión termina, la conexión se cierra.

El bloque de datos que pasa de TCP a IP, consiste en el encabezado TCP y datos de la capa de aplicación, esto es usualmente llamado un segmento.

Añade a los requerimientos de confiabilidad un número de facilidades:

- Detección y corrección de errores..
- Control de flujo.
- Secuenciamiento.
- Remover segmentos duplicados.

Detección y correcccion de errores. Se refiere a los segmentos que posiblemente han sido corrompidos por el medio físico o los niveles más bajos del software. El **control de flujo** es utilizado para prevenir una transmisión

excesiva hacía un receptor debido a las limitaciones de los recursos. El **secuenciamiento** es necesario porque la capa de IP puede liberar datagramas, llevando segmentos TCP, en cualquier orden; esto ocurre cuando los datagramas sucesivos utilizan diferentes rutas. El **duplicar segmentos** puede ocurrir por el mecanismo de recuperación de errores utilizados por TCP.

TCP añade todas estas facilidades para:

- Usar números de secuencia para identificar los datos.
- Reconocimientos positivos de datos recibidos en la secuencia correcta.
- Retransmisión de segmentos que no han sido reconocidos dentro de un tiempo límite (variable).

El mecanismo exacto será discutido a continuación.

III.4.5. TCP.

III.4.5.1. EL ENCABEZADO TCP.

Para proporcionar las funciones señaladas anteriormente, el encabezado TCP (Fig. 3.13) es mucho más complejo, con más campos que UDP. Así y por las mismas razones, el encabezado incluye los puertos origen y destino para identificar la aplicación. La mayoría de los campos restantes añaden confiabilidad y tratan con el control de la conexión.

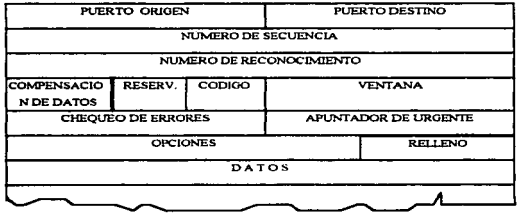

Fig. 3.13.- Encabezamiento TCP.

Número de secuencia - 32 bits. Como la mayoría de los protocolos que utilizan los números de secuencia para el control de errores, los números de secuencia se consideran como segmentos[2] que son transmitidos y recibidos.

[2] El segmento es un término TCP para la unidad de transmisión en esta capa de transporte. El término equivalente en otros protocolos es paquete o trama.

Pero con TCP, los números de secuencia en el encabezado de un segmento identifica la posición en el flujo de datos global del primer octeto de datos en ese segmento.

Sobre el establecimiento de la conexión, los nuevos números de secuencia son acordados por ambos nodos e inician la conexión. Para integrar un sistema después de que una máquina "se cae", los nuevos números de secuencia no inician en cero.

Si IP nunca libera datagramas en un orden diferente al que fueron transmitidos, los datos deberían llegar en secuencia y los números de secuencia se incrementarían ligeramente. El número de secuencia permite a TCP colocar un segmento dentro de la posición correcta en el flujo de datos, siempre que IP libere datos fuera de orden.

El número de secuencia es de 32 bits, así que aún cuando los enlaces sean rápidos toman como referencia el mismo valor del contador para que sea nuevamente válido y es muy grande. Esto significa que algún segmento recibido con el mismo número de secuencia como el de uno ya conocido, puede ser solo un duplicado, debido al proceso de corrección de errores. Los duplicados son permitidos y descartados sin alguna acción.

Número de reconocimiento - 32 bits. El número de reconocimiento avala la recepción correcta de todos los octetos hasta el número de reconocimiento menos uno. Cuando un transmisor de datos recibe un nuevo valor, puede

disponer de los datos que fueron guardados para su posible retransmisión. El número de reconocimiento sólo es válido si la bandera ACK está puesta.

Los números de reconocimiento, son respuestas a la recepción correcta de los números de secuencia y datos en secuencia desde el extremo remoto. Un número de reconocimiento, contiene el número de secuencia del octeto siguiente (en su flujo de datos recibidos que el transmisor pasará a su aplicación con el octeto "cero" numerado con los números de secuencia los cuales fueron intercambiados en el establecimiento de la conexión). Así que el número de reconocimiento es más grande que el número de octeto de último octeto en secuencia recibido. Esto es, por lo tanto, el mismo número de secuencia que estará en el siguiente segmento de datos a utilizar inmediatamente.

En TCP es posible enviar un número de segmentos que han sido recibidos correctamente pero que no han sido reconocidos porque el segmento crítico que está en la secuencia siguiente, ha fallado al llegar. También puede ser retrasado, porque fue enrutado por una trayectoria lenta o fue descartado por IP.

El número de reconocimiento no puede avanzar hasta que la pieza faltante del "rompecabezas" es proporcionado a través de la retransmisión dentro del tiempo límite.

Compensación de datos. Este mide la compensación al principio del campo de datos de aplicación en palabras de 32 bits. El valor normal es 5 cuando ninguna opción es utilizada.

Banderas. Las banderas son utilizadas para indicar la validez de otros campos y para el control de la conexión. Existen seis banderas separadas:

URG. Esta indica que el campo apuntador urgente es válido. Este campo señala a un octeto en el campo de datos que es el final de datos urgentes. Los datos urgentes no son considerados como parte del flujo de datos normal y deberán ser procesados antes que cualquier otro. Esta operación se utiliza en circunstancias donde un mensaje ha de ser pasado a través de la red hacia la aplicación. Este puede ser utilizado para interrumpir programas.

ACK. Esta bandera indica que el campo de reconocimiento es válido, el cual está en la mayoría de los segmentos. El campo de reconocimiento es normalmente inválido en la definición de la conexión antes de que cada nodo haya sido capaz de determinar que secuencia y valor de reconocimiento utilizar. El valor en el campo de reconocimiento puede no tener cambios entre segmentos, así, aunque el campo es válido puede no reconocer nuevos datos.

PSH. La bandera Push produce que la capa TCP remota pase este segmento inmediatamente a la capa de aplicación. TCP normalmente podría retener los datos más grandes para reducir el proceso de sobre encabezados, pero en algunas situaciones tales como una operación terminal de caracter-por-caracter, esto no puede ocurrir, aún si sólo un octeto de datos ha sido recibido.

RST. La bandera de reset es utilizada cuando todas fallan. Esta indica que ha ocurrido un error y que la conexión debe de ser cerrada forzosamente (o si se

envía como una respuesta a una requisición de conexión abierta, cuando la petición esta siendo rechazada).

SYN. La bandera de sincronía es utilizada al inicio del establecimiento de la conexión entre dos nodos. En esta etapa ningún extremo conoce que número de reconocimiento utilizar. Un establecimiento de conexión consiste de un intercambio en ambos sentidos de segmentos con la bandera de ACK puesta. La transferencia de datos puede entonces comenzar.

FIN. La bandera FIN es utilizada para terminar las conexiones. Cuando el extremo de una conexión no tiene más datos que enviar, este envía un segmento con la bandera FIN. Cuando ambos terminan y han enviado la bandera FIN la conexión se cierra.

Ventana - 16 Bits. La ventana indica la cantidad de espacio del buffer que el nodo tiene disponible para esta conexión. El otro nodo no debe enviar más datos que el indicado por el espacio del buffer.

Checksum - 16 Bits. El checksum TCP es un chequeo básico sobre el encabezado y datos. Este es calculado del mismo modo que en UDP, cada palabra de 16 bits se complementa a 1 y el resultado de la suma de estos complementos también es complementado a 1 tanto en el encabezado como en los datos.

Indicador urgente - 16 Bits. El valor en este campo apunta hacia el final de los datos considerados como urgentes y requieren atención inmediata. Este campo es válido solamente si la bandera URG está puesta.

Opciones - longitud variable. Hay solamente una opción normalmente usada con TCP la cual es el **tamaño del segmento máximo** (MSS). Este indica a la capa de destino TCP, el tamaño máximo del segmento (incluyendo el encabezado TCP) que deberá enviarse. El formato de esta opción se muestra en la Fig.3.14. El tipo 2 es la opción MSS; el tipo 0 y 1 son la lista de final de opción no operación, respectivamente. El campo de longitud indica la longitud en octetos del formato completo, esto es, incluye los campos de tipo y longitud.

Relleno. Si el campo de opciones es válido, el relleno asegura que los datos comienzan, en el límite del bit 32, así que la compensación de datos se puede indicar correctamente.

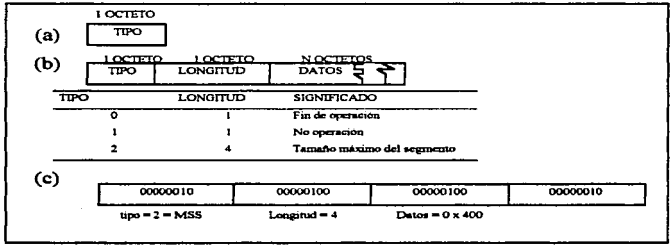

Fig. 3.14.- a) Formato de opciones b) opciones c) ejemplo.

En algunas implantaciones de TCP, MSS puede ser configurado para estipular el tamaño máximo de los segmentos aceptados por un nodo. Esto puede normalmente ser establecido a un valor máximo posible para reducir el encabezado de segmentos pequeños. Algunos equipos pueden estar restringidos en el tamaño de las tramas que estos pueden recibir, y por lo tanto necesitan establecer este valor, de tal forma que TCP no permitirá que los parámetros de las opciones excedan las capacidades del equipo.

La decisión para definir el tamaño de MSS es compleja. En un sistema que incluye ruteadores, ellos son requeridos para soportar una MTU de por lo menos 576 octetos, permitiendo un MSS máximo de 556. (576 menos el mínimo del encabezado IP de 20 octetos). Los segmentos más pequeños darán una respuesta rápida pero crea un rápido crecimiento de encabezados en la red, por lo tanto la eficiencia decrece, especialmente en conexiones de enrutamiento.

Tramas grandes mejoran la eficiencia pero al mismo tiempo incrementan los retrasos debido al tiempo que toman para llenar cada buffer. Si una trayectoria en la red tiene la tendencia a corromper tramas, entonces es probable que las más grandes sean corrompidas. Las tramas grandes aumentan la posibilidad de una retransmisión larga y de que el procesamiento en ruteadores y hosts comiencen con fragmentación y reensamble.

Con las mejoras en la tecnología WAN, la proporción de errores ha sido reducida significativamente, así que la proporción de pérdida o tramas corruptas también es reducida significativamente. Esto permite que segmentos

más largos que el tamaño máximo sean configurados. Solo en condiciones extremas serian necesario alterar estos valores desde el tamaño máximo posible.

III.4.5.2. TCP EN ACCIÓN.

Para explicar las caracteristicas de TCP, consideremos las fases de la conexión TCP. Veremos la conexión entre dos nodos, 128.1.0.1 y 128.1.0.9, donde 128.1.0.1 establecerá una conexión con 128.1.0.9.

III.4.5.2.1. FASE DE CONEXIÓN.

Para realizar una conexión TCP, está se inicia a través de una solicitud desde la capa de aplicación de algún nodo. En la figura 3.15. consideremos el nodo 128.1.0.1 solicitando una conexión con dirección IP 128.1.0.9 TCP envía entonces un segmento hacia IP que tiene la bandera SYN puesta, un número con un valor de secuencia en el campo (921) y la bandera ACK no puesta, lo cual denota que este es el segmento inicial de una conexión. En esta etapa, cuando el segmento se pasa a la capa IP, y si el nivel IP no tiene una entrada para la dirección IP 128.1.0.9 en su localidad ARP, puede realizar una solicitud ARP para obtener una dirección MAC del nodo 128.1.0.9. Una vez que se consigue la dirección MAC, el segmento es transmitido como un datagrama IP.

El nodo 128.1.0.9 responderá con un segmento similar al que tiene la bandera SYN puesta y la bandera ACK es puesta con su propio número de secuencia (302).

En el campo de reconocimiento, habrá un valor que es más grande que el número de secuencia enviado por el nodo 128.1.0.1 (921+1=303). Este segmento reconoce que 128.1.0.9 recibió el número de secuencia desde el nodo 128.1.0.1 y que propone su propio número de secuencia.

El Nodo 128.1.0.1 reconocerá que ha recibido la respuesta del nodo 128.1.0.9 para enviar un segmento que solo tiene puesta la bandera ACK y con un valor en el campo de reconocimiento que es en uno más grande que el número de secuencia enviado por el nodo 128.1.0.9 (302+1=303).
Una conexión TCP está ahora establecida; ambos nodos o extremos han intercambiado números de secuencia y están listos para enviar datos.

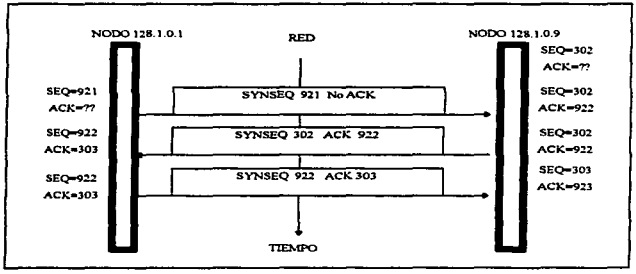

Fig. 3.15.- Puesta en fase de las conexiones TCP.

III.4.5.2.2. FASE DE DATOS.

Como el nodo 128.1.0.1 envía datos al nodo 128.1.0.9 el número de secuencia en el segmento apunta al primer octeto de datos transportado y la respuesta desde el nodo 128.1.0.9 deberá tener un número de reconocimiento que es en uno más grande que el número de secuencia recibido más el número de octetos llevado, esto es, el número de reconocimiento indica que octeto espera recibir el nodo 128.1.0.9.

Si la aplicación es un servicio de emulación de terminal que requiere eco de carácter desde la aplicación en el extremo remoto (nodo 128.1.0.9) los segmentos también tendrán puesta la bandera PSH. Esto impedirá que la capa TCP en ambos nodos retengan los datos y los forcé a pasar inmediatamente a través de la red y a la capa de aplicación así que los caracteres tendrán eco lo más rápido posible.

Esto continua hasta que todos los datos son enviados. Los reconocimientos son devueltos solo si hubo datos en el último segmento recibido, de otra forma el protocolo espera para el envío del siguiente dato. Los segmentos Keep-alive enviados por algunos protocolos para probar que una conexión sigue establecida, no son utilizados ya que ellos generan tráfico y este no es necesario para muchos sistemas.

Como cada segmento tiene el mismo formato para transmisión de datos o control , TCP puede reconocer los datos desde un nodo remoto y llevarlos en el

mismo segmento. TCP puede ser muy eficiente en el número de segmentos que usa. Para una conexión de Terminal usando Telnet con eco[3] desde un host remoto, TCP frecuentemente necesita solo tres segmentos por cada carácter escrito.

La Fig.3.16. muestra un ejemplo simple de TCP cuando una conexión de terminal tal como Telnet está operando con un host en modo eco.

Los caracteres tecleados por el usuario tienen que ser pasados a la computadora y regresar a la pantalla para ser desplegados. Ellos recorrerán la red dos veces, desde que el usuario oprime la tecla y el carácter es mostrado.

En este ejemplo el usuario a tecleado el carácter C que es enviado a través de la red con un número de secuencia 92. El sistema operativo regresa el eco del carácter y en la misma trama, el protocolo TCP reconoce la recepción de C desde 128.1.0.1. El nodo 128.1.01 entonces tiene que reconocer la recepción del carácter desde el 128.1.0.9, así un segmento de reconocimiento es regresado pero sin datos, el campo de reconocimiento comienza a colocarse mas allá de número de secuencia recibida. Esto es solo un carácter.

[3] El carácter de eco es utilizado por muchos sistemas interactivos. Cuando un carácter es escrito, no es mostrado sobre la pantalla local hasta que ha sido enviado de regreso desde un host remoto. Esto proporciona al host remoto la habilidad de decidir que quiere mostrar como respuesta de algún carácter. Al principio de la computación, esto fue utilizado como un método de chequeo de errores.

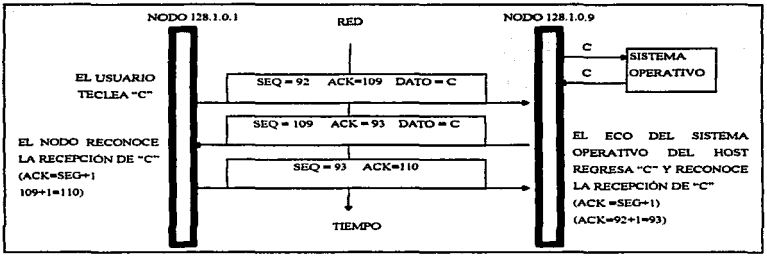

Fig. 3.16.- TCP realiza reconocimiento para un simple carácter con eco del host.

Con los sistemas que utilizan eco remoto, es posible que más de tres segmentos sean generados por cada carácter tecleado, si la computadora de destino esta con abundante carga. Esto sucede por que cada segmento lleva un carácter que debe ser reconocido dentro de cierto tiempo, de otra forma una retransmisión ocurrirá. Si la aplicación del host no está lista para regresar su respuesta dentro del periodo de tiempo este generara un segmento sin carácter de eco, pero con un reconocimiento de segmento entrante.

Cuando la aplicación está lista para regresar el eco del carácter hacia el transmisor, este enviará otro segmento y deberá recibir un reconocimiento desde la terminal de la computadora del usuario. En estas circunstancias, cuatro segmentos son generados en la (figura 3.17).

Cada segmento tiene un encabezado TCP, un encabezado IP y un solo carácter tecleado, formando 41 octetos en total, y es llevado en una trama del nivel de enlace.

Sobre Ethernet, cada trama deberá ser de un tamaño mínimo de 64 octetos[4], lo cual indica que para los 3 o 4 segmentos enviados por cada carácter tecleado por un usuario, 192 (64x3) o 256 (54x4) octetos son transmitidos entre el origen y el destino, dependiendo de la carga de la computadora remota. Así, cuando la computadora de aplicación es puesta bajo carga genera cuatro paquetes por carácter tecleado y estos ponen carga adicional en la computadora generando los extra reconocimientos.

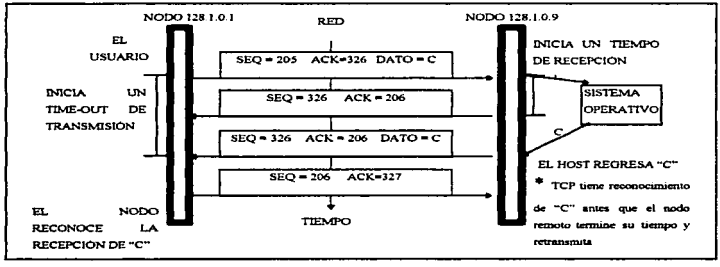

Fig. 3.17.- Cuatro paquetes por carácter debido a los retardos del host.

[4] Como el encabezado de la trama de Ethernet es de 18 octetos, cada trama lleva un carácter de escritura simple que puede ser rellenado por 5 octetos (18+41+5=64). Las tramas IEEE 802.3 no requieren relleno como LLC y SNAP añadiendo 8 octetos y creando una trama con un mínimo de segmentos TCP de 67 octetos (18+8+41=67)

El tráfico de red para esta aplicación se incrementa por encima del 33% porque la computadora esta cargada. La única forma para reducir el sobre encabezado causado por este problema es remover el "cuello de botella" en el host, el cual puede requerir un computador más grande; esto es que la computadora que está causando este problema está ejecutando lentamente sus tareas normales.

Un host que está con abundante carga a menudo enviará respuestas en segmentos múltiples, aunque una trama sencilla puede soportar la cantidad de datos que son transportados. Esto ocurre por que el software de comunicación usualmente corre en alta prioridad y genera tramas de salida en un tiempo establecido. Sobre una máquina ocupada, la aplicación no es capaz de ensamblar toda la información requerida antes de que el temporizador la anule.

Mientras que la operación de eco remoto puede ser aceptable sobre una red local con una capacidad de 7,000 a 14,000 tramas por segundo, el tráfico generado debe de ser cuidadosamente considerado cuando sea planeado un red WAN con puentes o ruteadores remotos. Si cada carácter tecleado genera tres o cuatro tramas, esto debe de considerarse cuando se dimensione la velocidad de los circuitos.

Por ejemplo, la capacidad de un circuito de 64 Kbps es alrededor de 120 tramas Ethernet de tamaño mínimo por segundo (en cada dirección). Si cada usuario teclea dos caracteres por segundo en promedio (20 palabras por minuto) cada uno puede generar cuatro tramas en cada dirección. La línea estará saturada en ambas direcciones por solo treinta usuarios activos. Las aplicaciones deben ser

modeladas individualmente y el tráfico que ellas generan debe ser considerado en cada punto de la red. El tráfico tiene dos parámetros: el número de bits por segundo requeridos y el número de paquetes o tramas por segundo.

Los "cuellos de botella" son mas probables en una red WAN.

La cantidad de tráfico producido por TCP puede parecer alta pero es menor a otros protocolos.

III.4.5.2.3. LA FASE FINAL.

En la fase final, cuando un extremo o nodo ha decidido cerrar la conexión, la bandera de FIN es utilizada. Para una conexión de terminal interactiva, el usuario probablemente registre su salida de la aplicación y esta le dirá a la capa de TCP que cierre la conexión. Esto causa que el modo de aplicación envíe un segmento con la bandera de FIN puesta. La bandera FIN le dice al nodo de la terminal responde con un segmento con ACK (para reconocer el FIN) y su propia bandera de FIN puesta. La conexión no es cerrada completamente hasta que ambos extremos han enviado un segmento con las banderas de FIN colocadas y posiblemente reconocieron que los segmentos de FIN fueron recibidos. Sin embargo si los segmentos se pierden en esta última etapa, la conexión será cerrada después de un corto tiempo fuera. En la práctica, cualquier extremo o nodo puede iniciar el cierre de una conexión con FIN.

En la Fig.3.18. el usuario ha finalizado su trabajo, así que ha escrito Logout para cerrar la conexión. Este mensaje es enviado al sistema operativo que libera la conexión la cual necesita ser cerrada. Nótese que el dato logout es reconocido como cualquier otro dato. Entonces el host cierra la conexión indicando al stack TCP que la conexión ha sido cerrada. Esto provoca que el software TCP envíe una trama con el código FIN. Si 128.1.0.1 decide que este ha terminado y no hay datos adicionales para enviar regresará un reconocimiento y un FIN los cuales indicarán al 128.1.0.9 de que la conexión está completa.

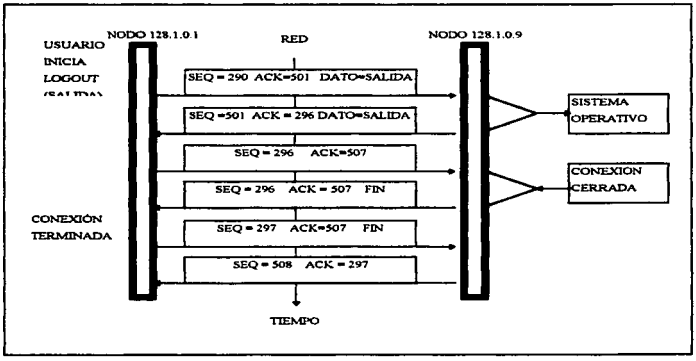

Fig. 3.18.- Etapa de cierre de una conexión TCP.

III.4.6. CORRECCIÓN DE ERRORES Y RETRANSMISIÓN TIME-OUT.

TCP proporciona la corrección de errores para aplicaciones TCP/IP que lo requiere. La arquitectura TCP/IP deja la corrección de errores a su nivel de transporte ya que desea que no existan suposiciones acerca de las capacidades de corrección de error en las capas bajas de la red.

Puesto que ha de ser corrección de errores para ciertas aplicaciones, ¿Por que no lo hace de una sola vez en los nodos terminales en la capa de transporte?. Esto significa que todas las correcciones de error en TCP/IP son asumidas de terminal a terminal[5] y no a intervalos, a diferencia de algunas redes, tales como implantaciones de X.25[6].

Existe un interesante manejo del efecto colateral de esta decisión.

Mientras no se determine como se debe realizar el manejo de errores en redes de capas, y si este manejo no es bueno, cualquier error sencillo querrá decir que un segmento TCP/IP es transmitido de terminal a terminal sobre cualquier enlace. En una red X.25 este habría sido transmitido sobre el enlace con error.

[5] Si TCP opera sobre una red de corrección de errores como X.25, muestra un sistema que es substancialmente libre de error pero que tiene cambios y retrasos en la operación del mecanismo de corrección de error.

[6] A diferencia de los autores de X.25, los diseñadores de TCP/IP estuvieron preparados para tener una muy buena visión del nivel de la aplicación requerida, ya que justamente designaron un nivel de servicio de red de transmisión que muestra al usuario ciertas garantías al llevarse a cabo.

Verdaderamente el mecanismo de corrección de error para TCP trabaja mejor cuando éste es requerido ocasionalmente. Afortunadamente, las tazas de error en circuitos de área amplia han sido perfeccionadas considerablemente con la introducción de sistemas de transmisión de fibra óptica, así que la decisión por los diseñadores de TCP/IP se justifica.

Para la corrección de errores TCP/IP usa un mecanismo sencillo: si un reconocimiento no ha sido recibido para algún número de secuencia de segmento en particular dentro de un cierto valor de time - out el segmento es retransmitido. Este es el único mecanismo para la recuperación de errores. A diferencia de algunos otros métodos de corrección de error, no hay forma de que un receptor pueda formar la retransmisión desde un punto en particular, aparte de que no existe el concepto de retransmisión de datos cuando se está fuera de secuencia. El receptor debe esperar la expiración del temporizador en el transmisor.

Ya que los segmentos son solamente reconocidos cuando están en secuencia, es probable que una vez que el tiempo de espera termina, una serie de segmentos serán retransmitidos. Esto es también posible en algunas implementaciones que retransmitiendo un sólo segmento provocará que un número notable de segmentos sean reconocidos. El estándar TCP puede acomodar ambos mecanismos. Lo que sucede en la practica, depende de como ha sido diseñada la implementación.

En la Fig. 3.19., un número de segmentos TCP han sido retransmitidos, ya que el último tamaño de la ventana anunciada a 128.1.0.1 permitió que la cantidad de datos fuera enviada. El segmento con número de secuencia 39 no logró alcanzar el destino, sin embargo, el último segmento lo logró (número de secuencia 49). TCP no reconoce el segmento con número de secuencia 49 dado que no ha recibido todos los datos intermedios. Esto provoca que el temporizador de retransmisión inicie desde el segmento con número de secuencia 39, ocasionando que el segmento sea retransmitido.

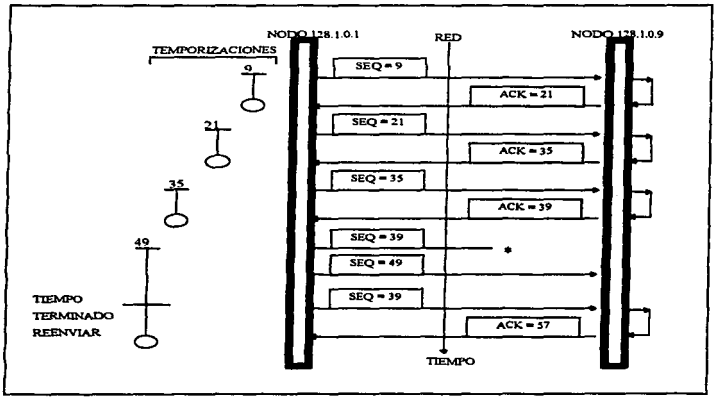

Fig. 3.19.- Un segmento que lleva datos falló al llegar.

En la Fig. 3.20., la pérdida del segmento de reconocimiento no requiere alguna acción adicional, como el segmento siguiente al reconocimiento perdido logro llegar, implica que todos los datos desde el número de secuencia 72 hacia arriba e incluyendo el segmento de datos con número de secuencia 170 han llegado a 128.1.0.9.

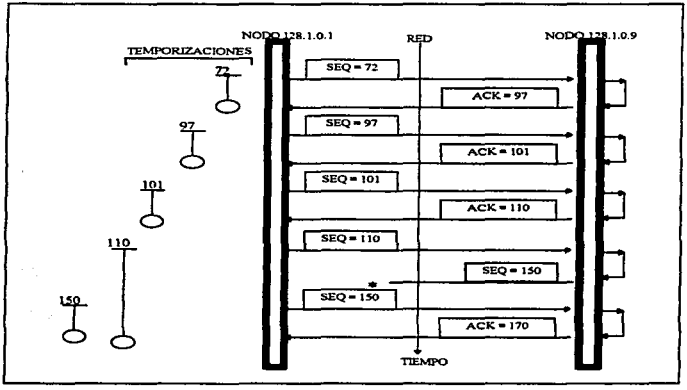

Fig. 3.20.- Reconocimiento de un segmento que falló al llegar.

El valor de la transmisión time-out es crítico. Este depende del retraso en el recorrido (RTT) de la trayectoria en uso.

Las LANs reconocerán en 20 a 100ms; las conexiones de área amplia sobre circuitos satélitales de baja velocidad pueden tomar algunos segundos. Es difícil reconocer anticipadamente las características del retraso en las redes, y pueden variar por un factor de 10 durante la vida de una conexión, dependiendo de la ruta y de la carga. Esto hace casi imposible de definir un valor de time-out para ese tiempo de retransmisión. Si el temporizador es determinado muy bajo, expirará antes de que el reconocimiento regrese, causando que el segmento sea enviado de nuevo innecesariamente e incrementando el tráfico. Si el valor se coloca muy alto, causa largos retardos esperando al vencimiento del temporizador antes de que la retransmisión pueda ser enviada, así que la pérdida de un segmento decrementará significantemente en la capacidad de la red.

Implantaciones modernas de TCP tienen una técnica que puede tratar con estas variaciones en posibles RTTs. Para solucionar el problema, todas las implantaciones de TCP utilizan un mecanismo que trabaja fuera del promedio de retraso de una conexión y añade un umbral sobre dicho retraso para manejar las variaciones. Un temporizador dinámico permite a una conexión cambiar su valor dependiendo de las circunstancias inmediatas y ayuda a construir un protocolo robusto. Esto minimiza el número de retransmisiones innecesarias mientras reducen el tiempo muerto, cuando se dan las retransmisiones.

Hay un número de versiones acerca de cómo este temporizador dinámico deberá ser implantado. Una de las técnicas más poderosas fue desarrollada por el uso en redes de paquetes por radio por Phil Kam. Esto exactamente considera

el tiempo de viaje redondo (RTT) de los segmentos perdidos. Este mecanismo ha sido ahora adoptado por algunas implantaciones comerciales de TCP/IP.

En las implantaciones de TCP un número de variantes de algoritmo de retransmisión son utilizadas, así que es importante entender las bases de los algoritmos time-out (temporizadores) y su estabilidad bajo gran carga y alta pérdida de segmentos.

Aún en la actualidad, no todas las implantaciones de TCP/IP utilizan algoritmos de time-out dinámico. Algunas tienen temporizadores fijos y otras tienen temporizadores que pueden ser configurados. En algunas implantaciones, diferentes valores de temporización pueden ser definidos para cada host. Ninguno de estos es tan satisfactorio como el temporizador dinámico a menos de que la topología de la red sea muy simple.

III.4.7. VENTANAS DE DESLIZAMIENTO, VENTANA DE AVISOS Y CONTROL DE FLUJO.

En redes que cuentan con altos retardos, los protocolos de reconocimiento positivo, pueden decrementar dramáticamente la capacidad de la red, cada segmento puede ser retenido, esperando los reconocimientos para viajar a través del sistema antes que el siguiente segmento pueda ser enviado. Un medio o enlace puede ser cargado solamente a una fracción de su capacidad, la cual decrece dramáticamente con el incremento del retardo del viaje redondo. Para

mejorar esto, TCP emplea un proceso conocido como ventanas de deslizamiento.

Las ventanas de deslizamiento permiten que múltiples segmentos sean transmitidos sin esperar el reconocimiento de cada segmento de manera individual. Si múltiples segmentos son recibidos en un nodo antes de que un reconocimiento este listo para enviarse, es posible reconocer el último segmento recibido, reduciendo así la necesidad de reconocer cada segmento. Esto permite tener una mayor capacidad y uso más eficiente del ancho de banda.

El uso de las ventanas de deslizamiento es particularmente importante en trayectorias a través de puentes y ruteadores, especialmente donde hay enlaces remotos.

Aún sobre una LAN la cual sólo puentes locales, los retrasos se crearán en los buffers de los puentes. Estableciendo el tamaño correcto de la ventana la operación se realizará casi como en una conexión directa. Las ventanas de deslizamiento, hacen a TCP (opuesto a UDP y otros protocolos LAN) particularmente bueno para operar en WAN's de larga distancia.

Un receptor tendrá espacio de memoria intermedia (buffer) limitado para cada conexión, así que debe de ser puesto un límite sobre la cantidad de información que puede ser enviada. Este límite es el tamaño de la ventana, la cual en TCP es medida en octetos. Existe una relación entre el tamaño de la ventana y el MSS.

Cuando un nuevo tamaño de ventana es proporcionado, es usualmente un múltiplo integral del MSS.

El tamaño de esas ventanas está normalmente en el rango de 1024 a 4096, el cual esta sólo entre uno y cuatro segmentos sobre una Ethernet con un MSS definido a 1024 y un MTU de 1500.

Un receptor de datos advierte un tamaño de ventana en cada segmento TCP que este envía. Cuando un dato no reconocido es el mismo como el tamaño de ventana advertido, no se envía más información hasta que un reconocimiento es recibido, el cual anuncia un nuevo tamaño de ventana de al menos un segmento máximo.

La ventana anunciada en cada segmento es un monitor útil cuando se están presentando dificultades de funcionamiento. Si los valores de la ventana son frecuentemente bajos o alcanzan cero en la mitad de la transferencia de datos, un dispositivo no tiene suficiente memoria asignada en los buffers. La ejecución puede ser mejorada si los buffers relevantes pueden ser incrementados.

Un receptor puede válidamente reducir el tamaño de la ventana a cero para detener completamente el flujo de datos, esto es, invocar al control del flujo. Esto es permisible sólo para reducir la ventana cuando es utilizada para validar datos sobre esta conexión. Un receptor no puede reducir una ventana previamente la cual ha sido llenada con datos.

Telnet utiliza control de flujo: cuando las teclas CTRL y' s' son presionadas al mismo tiempo en el teclado, esto detiene cualquier información adicional desde que ha sido desplegada en la pantalla de esa terminal. CTRL y' s' generan el carácter ASCII DC3 o XOFF. En este evento, un servidor de terminal Telnet operando sobre TCP tiene que detener la transmisión desde el host remoto para prevenir el sobreflujo en los buffers del servidor terminal, de otra forma los datos se perderán. Si los datos continúan recibiéndose y llenan la ventana de advertencia previamente, TCP envía segmentos reduciendo los tamaños de ventana hasta que finalmente alcanza cero. Si el flujo de datos es rehabilitadoi con CTRL y' q' juntos (el carácter ASCII DC1 o XON), los datos empezarán a fluir hacia la terminal nuevamente, los buffers serán liberados y los segmentos hacia el host remoto indicarán el incremento de tamaño de la ventana del servidor terminal. Por eficiencia, una ventana nuevamente anunciada, siempre debe ser por lo menos de un segmento máximo.

En la Fig. 3.21., el ejemplo muestra una conexión donde los buffers están saturando el nodo 128.1.0.9 así que la ventana ha elegido a 200 octetos y de allí a 0. Cuando 128.1.0.9 esté disponible para tratar con los datos que éste recibe, limpiando efectivamente los buffers receptores, advierte nuevamente una ventana de 1024, así que los datos comienzan a fluir de nuevo.

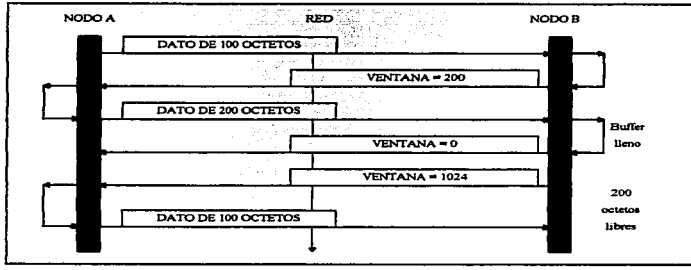

Fig. 3.21.- Ventana de advertencia en TCP.

IV. APLICACIÓN.

IV.1. MODELO CLIENTE/SERVIDOR.

Los servicios en el nivel de aplicación de TCP/IP a menudo son referidos a que tienen una relación de **cliente/servidor** (Fig.4.1.). Esto significa que un servicio en el nivel de aplicación consiste de dos partes complementarias, una en cada uno de los nodos intercambiando información. La parte originante de una conexión es llamado el **cliente** y la parte receptora el **servidor.**

Un servidor en el nivel de aplicación espera las conexiones de entrada o **solicitudes.** El cliente realiza las conexiones o solicitudes a los servidores si así lo requiere. Una vez que la conexión se establece y queda abierta, el cliente realiza solicitudes y el servidor le da las respuestas o contestaciones a esas solicitudes. El servidor no inicia una transacción. El software del servidor no puede comunicarse directamente con el sofware del cliente. Así, para establecer conexiones y transferir información, debe existir el software de operación del cliente y del servidor en el nivel de aplicación.

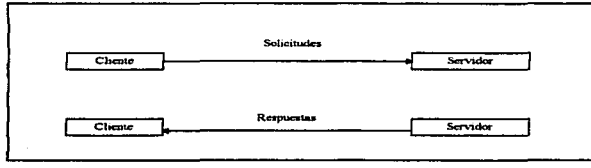

Fig. 4.1.- Arquitectura Cliente/Servidor.

Puesto que la aplicación del servidor es software, una computadora con un sistema operativo que soporta multitareas (OS/2, UNIX O VMS por ejemplo) puede tener muchos tipos diferentes de software de cliente y servidor ejecutándose al mismo tiempo. Así, esas computadoras multitareas pueden manejar múltiples conexiones dentro de sus servicios y realizar conexiones hacia otros servicios de computadoras y que externamente aparecen como una relación directa, de usuario, pero cada conversación se basa en una arquitectura de cliente/servidor.

Por tanto, se requieren dos diferentes piezas de software para permitir la comunicación. Por ejemplo, si usted estuviera utilizando una terminal Telnet, ambas, la computadora local que estuviera utilizando y la computadora remota con la que se estuviera comunicando, solicitarian Telnet, pero usted solicita el cliente Telnet y el host final solicita el servidor Telnet. Esto es cierto para FTP, TFTP y BOOTP; en efecto, muchos servicios TCP/IP operan de este modo.

Debido a lo estrecho de la relación de UNIX con TCP/IP, el software del servidor a menudo es referido como un **daemon**, asi al servidor Telnet usualmente se le llama **telnetd** (se pronuncia " telnet -dee "), que significa Telnet daemon, y al servidor FTP se le llama ftpd y así sucesivamente. Para una conexión de trabajo entre dos nodos, uno debe tener Telnet y el otro telnetd, o uno debe tener FTP y el otro ffpd. La Tabla 4.1. enlista algunos módulos software cliente/servidor.

Cliente	Servidor	Puerto	Descripción
Telnet	telnetd	23	Servicios de acceso terminal
FTP	ftpd	20/21	Servicios de transferencia de archivos
LPR (721-731)	lpd	515	Servicios de impresión remota
SMTP	dmtpd	25	Servicios de correo electrónico
rlogin	rlogind	513	Servicios de login remoto

Tabla 4.1.- Módulos software cliente/servidor.

IV.2. APLICACIONES EN TELNET, FTP, SMTP Y X WINDOWS.

IV.2.1. TELNET.

Antes que la PC llegará a ser tan común, los usuarios se conectaban a una computadora utilizando una terminal tonta. La terminal proporciona un teclado y una pantalla por donde se presentan los programas que se ejecutan en la computadora-también-llamado trabajo interactivo. Las redes de computadoras de datos crecieron tanto como los usuarios desearon tener acceso a muchas computadoras sin tener una conexión separada para cada una. Telnet fue diseñada para proporcionar este servicio, permitiendo a los usuarios accesar a todas las computadoras que estaban conectadas a la "red". El host remoto se pereceria a ellos, desde su host local, como si estuvieran ligados directamente a ésta. Ellos usarían comandos estándar en su máquina local para accesar a cualquier tipo de computadora.

Telnet es un acceso terminal interfase del nivel de amplificación. Proporciona soporte de acceso terminal para terminales todas comunicándose con hosts remotos. Estas terminales pueden conectarse de tres maneras como:

(1) terminales conectadas a Telnet TCP/IP " servidores terminales"

(2) terminales directamente conectadas a hosts ejecutándo TCP/IP

(3) PC's ejecutando una emulación de terminal y software TCP/IP

IV.2.2. EL PAPEL DE TELNET.

La princcipal funcionalidad que Telnet proporciona es la compatibilidad entre sistemas de computadoras de modo que las aplicaciones cliente final logren acceso terminal hacia el host final-servidor remoto sin tener conocimiento de como soportar cualquier tipo de terminal en particular. El uso específico es permitir a las terminales remotas conectarse a un host servidor de aplicaciones, puede ser a través de una computadora intermediaria y aparecer como si fueran terminales conectadas directamente a ese host.

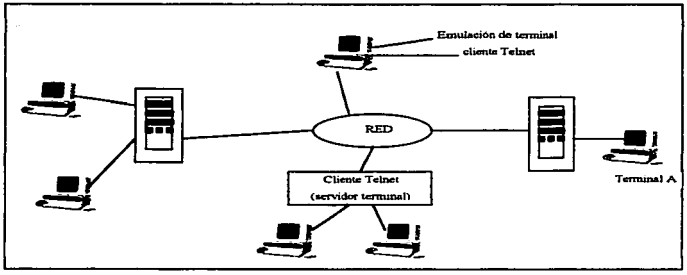

Fig. 4.2.- Arquitectura Telnet.

El servicio que los usuarios ven es el servicio terminal del host remoto. Una vez conectados, son validados por las identidades de usuario y claves de acceso y entonces tienen acceso permitido a aplicaciones autorizadas. El servicio remoto es representado de la mejor manera posible en su pantalla terminal local. Ellos deben saber como operar una terminal de la computadora que ellos accesen.

El servidor Telnet tiene que hacer una conexión de cliente Telnet parezca como cualquier otro usuario del sistema operativo del host por la activación de todos los programas de validación necesarios y crear un ambiente para cada conexión lógica hecha a éste. Una vez que el usuario sale de la computadora host del servidor Telnet, es también responsable de terminar la conexión lógica que tenía lugar a través de la red.

En la Fig. 4.2. todos los usuarios son capaces de accesar al host A con la misma funcionalidad como si estuvieran conectados directamente al host, como lo está la terminal A. Para que una conexión aparezca en el host como si ésta fuera una terminal enlazada directamente, se requiere de un protocolo confiable, asi Tenet opera con TCP.

IV.2.3. PROTOCOLO DE TRANSFERENCIA DE ARCHIVO FTP.

Es común desear transferir archivos entre diferentes tipos de computadoras, pero hacer esto implica tratar con una serie de problemas. Mover los datos es franco, pero ¿ qué sucede cuando estos arrivan ? Los principales problemas son que las computadoras almacenan datos en diferentes formatos, sus sistemas operativos utilizan diferentes comandos para funciones similares y tienen diferentes restricciones de seguridad para prevenir accesos no autorizados a programas y datos. Estas consideraciones se aplican a los archivos de datos.

FTP fue diseñado para proporcionar un servicio de aplicaciones que querian mover archivos entre redes de computadoras. Este proporciona los servicios básicos en la capa de aplicación necesarios para mover archivos; éste no define la interfase para un usuario, por consiguiente una aplicación de usuario y FTP. Aunque usted invariablemente escriba "FTP" para realizar una transferencia de archivo, está usted invocando un programa interfase así como al software FTP pertinente.

Como un servicio termina, un servicio de transferencia de archivo no debe introducir errores. FTP requiere un servicio de comunicaciones confiable, por tanto, éste utiliza el servicio de transporte TCP.

La función principal de FTP es reducir o remover las incompatibilidades entre el manejo de archivos en diferentes sistemas operativos. Por ejemplo, si usted se conecta a una computadora remota, su primera solicitud podría ser una lista de todos los archivos en un directorio. Los comandos para haceresto difieren para diferentes sistemas operativos (Tabla 4.2).

Enlistar un directorio es parte de la administración de archivos. Así como la transferencia de archivos, FTP debe proporcionar las funciones básicas de manejo de archivos de una manera estánda. Cuando un usuario en un sistema operativo de una computadorautilizando un sistema operativo diferente, el comando para enlistar un directorio requiere de traducción. Esto es cierto para muchas otras funciones, tales como cambiar de directorio, login, crear un directorio, borrar un archivo y así sucesivamente.

Sistema Operativo	Comando de directorio
	dir
	dir
	(click on folder)
	ls
	(Double click on folder)

Tabla 4.2.- Enlistando un directorio.

Una principal facilidad de FTP es, por tanto, tratar con la traducción necesaria para proporcionar compatibilidad entre diferentes sistemas operativos. La manera en que FTP hace esto a través de lo que se define como **comandos estándar de red**. Una lista estándar de funciones comunes está definida para FTP para asegurar que, sin hacer caso del sistema operativo, el comando que pase a través de la red es siempre el mismo.

La Fig. 4.3 muestra conceptualmente como FTP trata con esta traducción. En este ejemplo, un usuario MS-DOS está comunicándose con un sistema operativo UNIX. El usuario de sistema MS-DOS desea ver una lista de todos los archivos en el directorio en la computadora remota. En una PC basada en MS-DOS el usuario instintivamente usaría el comando normal para enlistar un directorio con MS-DOS. El cliente FTP convierte esta solicitud en un comando FTP el cual es LIST. LIST es el comando FTP estándar desde el cliente FTP hacia un servidor FTP para solicitar una lista de directorio. Cuando el software servidor recibe el comando, éste realiza lo nacesario en comandos UNIX para conseguir una lista de directorio y entonces lo regresa a la salida del cliente.

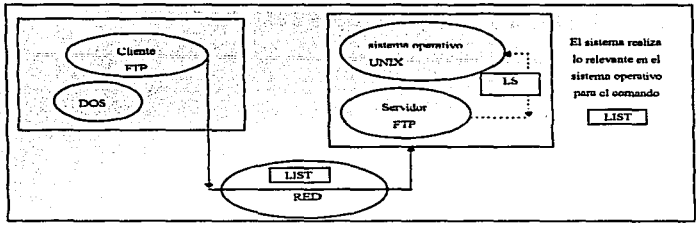

Fig. 4.3.- Traducción de comandos FTP para enlistar un directorio.

La Tabla 4.3. muestra una lista de los comandos FTP estándar. Estos comandos son los actuales caracteres superiores ASCII enviados a través de la red en el campo de datos de los segmentos TCP. En las práctica, pueden ser vistos en texto con un analizador de red y como son transmitidos. Esto puede ser una ayuda potencial para resolver las incompatibilidades entre implementaciones.

La lista de comandos de la Tabla 4.3. no está completa, pero estos son los más comunes proporcionados para muchas implementaciones. Conocer estos comandos no tiene un valor para el usuario; sólo son utilizados por el cliente FTP y el software servidor para comunicarse uno con otro.

USER (userind) <cr,lf>	Identidad del usuario con acceso
PASS (password) <cr,lf>	Clave de acceso del usuario
ACCT <cr,lf>	Información de cuenta
CWD (directory) <cr,lf>	Cambiar directorio de trabajo
CDUP <cr,lf>	Cambiar al directorio raiz
QUIT <cr,lf>	Salir de FTP
PORT (socket) <cr,lf>	Definir el puerto a utilizar
TYPE type <cr,lf>	Definición de TYPE
RETR (filename) <cr,lf>	Recuperar un archivo
STOR (filename) <cr,lf>	Enviar un archivo
DELE (filename) <cr,lf>	Borrar un archivo
RMD (directory name) <cr,lf>	Borrar un directorio
MKD (directory name) <cr,lf>	Crear un directorio
LIST (directory name) <cr,lf>	Lista directorio de usuarios
NLST (directory name) <cr,lf>	Lista directorio de programas
STAT <cr,lf>	Estado
HELP <cr,lf>	Ayuda

Tabla 4.3.- Comandos FTP cliente/servidor.

IV.2.4. PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO SMTP.

Por muchos años, el deseo de utilizar correo electrónico ha sido intenso. Este puede dar un rapidísimo vuelco en torno al entonces tradicional correo y puede ser utilizado en muchos sistemas de computadoras. Los sistemas de correo pueden ser aumentados para proporcionar servicios amigables tales como envío

de correo a grupos de usuarios, permitir a los procesadores de palabra transmitir sus archivos automaticamente, enviar documentos con el correo como enlace o correo manualmente registrado asi esto es posible saber siempre y cuando el receptor haya leído un artículo.

El correo es el nivel de aplicación de TPC/IP ha ayudado indudablemente al desarrollo del sistema TCP/IP en si mismo para permitir que la información y las ideas se transfieran libremente por toda la red internet como redactar RFC's.

SMTP es un servicio que permite que el correo de paquetes se comunique con algún otro entre diferentes computadoras. Como su nombre lo indica, es un protocolo simple. Este opera de manera similar a FTP. El cliente envia comandos basados en ASCII al servidor y el servidor responde con respuestas númericas y de texto como se muestra en la Fig.4.4. Recuerde, tales comandos son pensados para usarse entre el cliente SMTP y servidor, no para usuarios finales.

Las solicitudes y respuestas mostradas en la Fig.4.4 son transportadas en el campo de datos de TCP, en ASCII, así un analizador de red es capaz de desplegar estas transacciones muy facilmente. Muchos sistemas de correo tienen una opción debug para ayudar a analizar problemas. Permite la inspección de las transacciones y como se transfieren entre el cliente y el servidor.

Comandos del cliente	EXPLICACIÓN:
Comando	Una conexión es solicitadad desde el sistema de
HELO <trining>	entrenamiento.
MAIL FROM: <JIM:@Training.edu>	Desde Jim en el sistema de entrenamiento
RCPT TO: <Kevin@Sales.com>	Enviar a Kevin en el sistema de ventas
DATA	El texto DATA termina con <cr,lf>,<cr,lf>
QUIT	Terminar esta conexión
RSET	Abortar esta conexión
NOOP	Ninguna operación

Respuestas del servidor
250 OK
251 Usuario no local; avanzar hacia <dondequiera>
550 Acción requerida no tomada; buzón no disponible
354 Iniciar entrada al correo; finalizar con <cr,lf>, <cr,lf>
500 Error de sintaxis

Fig. 4.4.- Comandos y respuestas SMTP.

IV.2.5. Protocolo X.

Con la reciente demanda de aplicaciones windows - aplicaciones que operan a través de una interfase de Usuario Gráfico (GUI) - una interfase de programación estándar que proporciona compatibilidad entre diferentes sistemas hardware es una adición muy útil para el nivel de aplicación. Para encontrar este requerimiento el Sistema X Window se esquematiza en la recomendación RFC 1013 y por consiguiente se puede ver como un estándar " abierto ", aún cuando este es desarrollado por MIT.

La operación del Sistema X Window no está atado a algún protocolo en particular, pero ha sido predominantemente utilizado como UNIX y por

consiguiente en TCP/IP, así que X Window ha llegado a asociarse con TCP/IP. La definición del Sistema X Window considera un programa que consiste de módulos cliente y servidor que se pueden localizar en alguna máquina o en diferentes máquinas a través de una red. La definición de cómo los programas cliente y servidor se intercomunican se define por un protocolo llamado **Protocolo X.**

El Sistema X Window lleva un largo camino proporcionando computadoras con estandares para accesar aplicaciones sobre diferentes arquitecturas de computación. Esto es porque está mucho más involucrado en la representación de datos para usuarios de computadoras que en las técnicas más recientes; éste proporciona una interfase estándar entre la interfase de usuario de verdad y el software remoto que maneja esa interfase estándar, cualquier aplicación que genera el protocolo X como salida, sin tomar en cuenta que hardware o sistema operativo de la aplicación esté ejecutandose.

Cuando se discute X Window, uno debe ser cuidadoso con los términos servidor y cliente. Aquí el servidor es un programa que controla el despliegue de información para usuarios; el cliente es una aplicación que genera esa información (Fig. 4.5.). Las terminales X son dispositivos especificos y estaciones de trabajo inteligentes dedicadas a la tarea de ser un servidor X Window. Tal como el nombre sugiere, el Sistema X Window se basa en un ambiente de ventanas GUI en dónde el mouse y los menús son adiciones importantes del teclado que proporcionan la interfase de usuario. Todo esto está asociado con el servidor X.

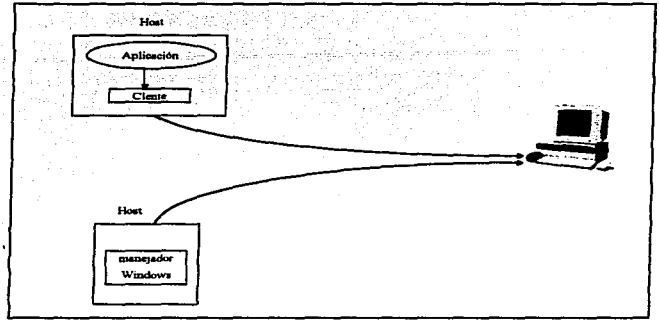

Fig. 4.5. Arquitectura del sistema X Window.

En una arquitectura cliente/servidor, el servidor normalmente solo responde a las solicitudes del cliente. Dentro del ambiente X Window, los movimientos del mouse y los teclados son reportados al cliente a través de comandos de evento.

El Sistema X Window ha llegado a ser un importante vehículo en la plataforma hacia la compatibilidad. Esto es porque cualquier aplicación que puede operar como cliente X puede ser utilizado por un servidor X sin tomar en cuenta que computadora o sistema operativo pueden estar utilizando. Lo que se requiere es una red de conexión común y un protocolo tal como TCP/IP.

El protocolo X es una definición completa de funciones que soportan el mouse, entradas de teclado, producción de ventanas, cajas, lineas, círculos y de hecho cualquier cosa que se haga con dibujos y texto en windows sobre una pantalla.

El protocolo utiliza TCP como un flujo de transporte confiable. Este abre un puerto separado para cada ventana iniciando con el puerto 6000 y agregando un 1 para cada subsecuente ventana. Hay cuatro diferentes tipos de mensajes utilizados por el protocolo X: solicitudes, respuestas, errores y eventos.

En su forma básica, cada evento pasa a través de la red entre servidor y cliente. Moviendo un mouse sobre una pantalla de X Window puede generarse un flujo de tráfico en la red. Tal actividad solo es práctica en un ambiente verdaderamente local. Cambios recientes a la definición de X Window apuntan en cambio a la división de actividades entre el cliente y el servidor; esto permite al servidor localizar más procesos en pantalla y reducir el tráfico entre dispositivos a niveles aceptables sobre otros tipos de enlace.

IV.3. SISTEMA DE ADMINISTRACIÓN DE RED.

En adición a los protocolos que proveen servicios a nivel de red y programas de aplicación que usan esos servicios, una red internet necesita software que permita a los administradores depurar problemas, controlar ruteo y encontrar computadores que violen los estándares del protocolo.

La administración de red es un problema clásico de tecnología de información. Una gran cantidad de información detallada se requiere para entender que está sucediendo dentro de un sistema, la cual, una vez procesada permite tomar decisiones necesarias sobre cómo controlar, adaptar y desarrollar el servicio.

El Protocolo Simple para la Administración de Red (Simple Network Management Protocol, **SNMP**) es un protocolo para el monitoreo de rede bajo TCP/IP y que ha gozado de una gran aceptación a nivel comercial. Existe una gran diversidad de paquetes de administración comerciales que emplean SMNP como norma, tales como Netcentral Station de Cisco, SPECTRUM de Cabletron y Network Management de Synoptics entre otros.

La historia de SNMP es interesante porque refleja muchas de las diferencias entre el desarrollo de OSI y TCP/IP, SNMP fue definido originalmente para usarse con TCP/IP pero fue basado en definiciones OSI para la administración de la red. El término SNMP es comúnmente utilizado para referirse al grupo completo de los componentes necesarios para administrar una red. SNMP es el protocolo utilizado para manejar información de administración entre dispositivos de una red, no cubriendo esta definición todos los aspectos del sistema.

El SNMP está formado por una serie de componentes, los cuales se definen acontinuación:

- *Administrador.* Es el programa que reside en la estación central de administración de red. Tiene la capacidad de encuestar a sus agentes utilizando los comandos propios del SNMP.

- *Agente.* Es un programa que recide dentro de todos los dispositivos a administrar: computador, concentrador, puente, ruteador. Este programa captura y almacena la información de los dispositivos, respondiendo a las peticiones del programa administrador.

- *MIB.* La base de Información de Administración es una base de datos virtual de objetos manejables como dirección de red, tipo de interfase, contadores, estando accesible al agente y puede ser manipulada por los comandos SNMP.

- *Comandos de Operación.* Serie de comandos que permiten interactuar con los agentes y bases de datos.

- *Agentes PROXY.* Agente con un programa especial para convertir protocolos de otros sistemas de administración (propietarios). Facilita la migración hacia SNMP y permite administrar dispositivos que no manejan SNMP.

El funcionamiento de SNMP es relativamente sencillo: Los agentes tienen la capacidad de captar y guardar la información requerida para la administración de red, apoyándose con los datos de MIB. El Administrador obtiene la información de los agentes por medio de los comandos de operación.

Como se observa, uno de los objetivos de SNMP es recolectar la información de administración en los dispositivos de la red y centralizar el análisis complejo.

El aspecto más significante de SNMP es el poder que proporciona para monitorear y controlar redes. La simplicidad de SNMP y su efectividad lo ha ubicado como un vehículo para el desarrollo de mecánismos altamente sofisticados para controlar sistemas de red.

El SNMP fue diseñado en base a OSI con un deseo de producir un sistema práctico que pudiera económicamente ser integrado a todos los nodos dentro de una red. Como un resultado, SNMP es un sistema de administración orientado a no conexión, diseñado para operar sobre la capa de transporte UDP de TCP/IP.

CONCLUSIONES.

Trataremos ahora sobre las futuras direcciones que Internet y TCP/IP pueden tomar, así como su impacto en la interconexión de redes en general.

El incremento de interés y participación en Internet en los últimos años es sorprendente. En 1989 hubo un estimado de 1,200,000 conexiones en Internet a lo ancho del mundo. Al inicio de 1991 hubo más de 1,000,000 de conexiones y la tasa de crecimiento sigue aumentando.

Gran parte del interés sobre Internet se desprendió de las fallas que tuvo OSI para desplegarse satisfactoriamente. En 1989 el gobierno federal de los Estados Unidos mandó que todas las computadoras tuvieran OSI presente en su sistema. No tenía que correr, solo estar presente. En 1990 el requerimiento fue que todas las nuevas computadoras corrieran OSI. Sin embargo, siguieron los problemas principalmente con los tiempos de respuesta y carencia de aplicaciones para correr en el sistema. Las necesidades de interoperatividad seguían incrementandose.

Así, mientras los departamentos y agencias vacilaron sobre que hacer para tener OSI en línea en cualquier lugar, un viejo protocolo fue 'descubierto'. TCP/IP estuvo presente y funcionando, pasando a ser súbitamente una solución hasta que OSI estuviera disponible.

Con el gran interés que surgió en el gobierno de Estados Unidos, la industria comenzó a ver a TCP/IP como una manera de resolver sus problemas. Así más y más desarrolladores sacaron sus productos al mercado para soportar este interés de la industria.

TCP/IP no requiere de alguna interfase física en particular ni de alguna clase de host en especial para trabajar. Con estos dos factores en su favor, éste se puede considerar como el punto de enganche entre los primeros protocolos portadores y cualquier nuevo sistema de comunicaciones o hosts.

El futuro comercial de las aplicaciones y comunicaciones computacionales estará cerca de mezclar técnicas TCP/IP y OSI existentes y futuras. Pero esto pasará solamente si las normas OSI están superando las limitaciones TCP/IP o proporcionando facilidades útiles que no estén disponibles en otras técnicas. Esto significa que las aplicaciones OSI deben comenzar a entregar un ambiente más poderoso en funciones.

Por lo pronto, el gobierno de Estados Unidos ha definido un plan para migrar de TCP/IP a OSI, conforme las capacidades de OSI vayan madurando y estén disponibles. De una manera general, los pasos serían los siguientes:

- **Fase 1:**

  TCP/IP y OSI corren en redes separadas

- **FASE 2:**

  TCP/IP y OSI se comunican uno con otro a través de un gateway, conformando la misma red física

- **Fase 3:**

  OSI trabaja con TCP/IP en la misma red a través de software TCP/IP de equivalentes OSI. Disminuye la utilización de los gateways.

- **Fase 4:**

  OSI proporciona mayores facilidades que TCP/IP y éste comienza a ser obsoleto.

- **Fase 5:**

  Finalmente, las redes trabajan completamente con OSI utilizando la vieja red física de Internet.

En la fase 1 y 2 opera en modo limitado, usado principalmente para aplicaciones experimentales y pruebas.

En la fase 3, OSI está a nivel de TCP/IP y las comunicaciones OSI usan los equivalentes TCP/IP para los mensajes desde y hacia los hosts TCP/IP. Esto es el modo equivalente OSI.

Desde la fase 4, OSI se dice estar en el modo avanzado y proporciona servicios y facilidades mejores que las que proporciona hoy en día TCP/IP.

Cuando la fase 4 esté completa para OSI, el final de TCP/IP estará cerca. Este se unirá a la serie de protocolos precedentes y se desvanecerá en la historia de la comunicación de datos tal como BSC, PARS, SABER y muchos otros. TCP/IP ha vivido más allá de lo esperado y en estos años de auge sigue con todo su potencial proporcionando un puente desde Internet hacia un OSI global.

B I B L I O G R A F I A.

Redes de computadoras. Protocolos, normas e interfaces.
Uyless Black
Macrobit
1990

TCP/IP running a successful network
K. Washburn, J. T. Evans
Addison-Wesley
1993

Internet Working with TCP/IP, Volume I.
Principies, protocols and architecture
Second Edition
Souglas E. Comer
Prentice Hall
1991

Seminario TCP/IP
IBM Corporation
1992

Seminario Práctico Interconexión de redes con TCP/IP
Teledata
Revisión 2.5
1992