UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

"TELEFONÍA DIGITAL Y RDSI"

"PROTOCOLOS TCP/IP"

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A :

JOSÉ LUIS RAYGOZA GALVÁN

ASESOR: ING. VICENTE MAGAÑA GONZÁLEZ

CUAUTITLÁN IZCALLI, ESTADO DE MÉXICO 2003

PAGINACIÓN DISCONTINUA

UNIVERSIDAD NACIONAL AVANZADA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN. Q. Ma. del Carmen Garcia Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario

Telefonia Digital y RDSI
"Protocolos TCP/IP"

que presenta el pasante: José Luis Bayoza Galván
con número de cuenta: 08818760-8 para obtener el título de
Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 21 de Noviembre de 2002

MODULO	PROFESOR	FIRMA
IV	Ing. Vicente Magaña González	
I	Ing. José Luis Rivera López	
III	Ing. Víctor Hugo Arroyo	

B

AGRADECIMIENTOS

A DIOS .....

PORQUE SIN ÉL, SU AMOR Y SUS CUIDADOS, NO HABRÍA LOGRADO CUMPLIR ESTA META.

A MIS TIOS.....

HILDA GALVAN Y FRANCISCO ESCOBAR, PORQUE SIEMPRE ME HAN APOYADO.

A MIS PRIMOS.....

ROBERTO, CRISTINA Y AMPARO, POR SUS CONSEJOS Y TODO SU APOYO.

A MIS FAMILIARES Y COMPAÑEROS.

POR LA MOTIVACIÓN Y CONSEJOS, ASI COMO EL APOYO HACIA A MI EN EL TRANSCURSO DE MIS ESTUDIOS.

A MIS PADRES.....

(†) J. SANTOS RAYGOZA Y MATILDE GALVAN, POR TODO SU AMOR, SACRIFICIOS Y HABER CREIDO EN MI.

A MIS HERMANOS .....

MARTHA, JORGE, ILDEFONSO, MARCO ANTONIO Y ANA LAURA, POR SU APOYO Y MOTIVACIÓN PARA SEGUIR ADELANTE.

A MIS PROFESORES.....

POR LA ENSEÑANZA QUE ME BRINDARON EN EL TRANSCURSO DE MIS ESTUDIOS.

Y A TODAS AQUELLAS PERSONAS QUE SIEMPRE ME MOTIVARON PARA MI FORMACIÓN PERSONAL.

GRACIAS

PREFACIO

La computadora ha evolucionado hasta convertirse hoy en día, no solamente en un dispositivo de almacenamiento y procesamiento de información, sino en un medio de comunicación.

Las compañías telefónicas dependen para el desempeño de sus funciones de equipo de cómputo para manejar las cuentas de los consumidores, la realización de diagnósticos y mantenimiento de la red; les brindan auxilio en el control de llamadas telefónicas, sus tarifas y enrutamiento.

Gracias a ellas se ofrecen una enorme variedad de servicios, tales como servicio de voz que incluye marcación, llamada activada en tres sentidos, mensajes controlados por voz e Internet.

El caso de Internet es ilustrativo de la capacidad de interacción que se ha obtenido utilizando la computadora y las redes de telecomunicaciones.

A través de Internet viajan miles de millones de bits con información proveniente de todo tipo de fuentes: sonidos, imágenes, textos, archivos de computadora, transacciones bancarias, paquetes de programas, correo electrónico, consultas a bancos de información o a bibliotecas, compras a distancia, aplicaciones de multimedia. Aunque habrá que trabajar arduamente en la definición de los mecanismos de acceso, de control y de conmutación más eficientes, así como en la definición de las arquitecturas de red más adecuadas para lograr transmisiones a las velocidades que se requieren para los servicios que se desean prestar, se puede ver que ya se tiene un enorme trecho del camino recorrido.

En este trabajo vamos a estudiar el modelo de referencia OSI y el modelo del protocolo TCP/IP. El primero es un modelo teórico de arquitectura de red, independiente de los protocolos usados, que es la base de estudio para el diseño y entendimiento del trabajo en red, mientras que el segundo es un modelo práctico, implementado en la actualidad a nivel mundial, siendo el soporte no sólo para la intercomunicación de todo tipo de redes, si no también la base sobre la que se ha desarrollado la red mundial de las comunicaciones: Internet.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.

- Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Aunque el modelo de referencia OSI es universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el **TCP/IP** *(Protocolo de control de transmisión / Protocolo Internet)* . El modelo de referencia TCP/IP y la estructura del protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio.

El Modelo TCP/IP se basa en el tipo de conmutación de paquetes y su estructura esta formada por las Capas de Aplicación, Transporte, Internet y Red.

El Modelo TCP/IP tiene algunas capas con el mismo nombre que las del modelo OSI, cada una de estas tiene diferentes funciones, por lo que no deben confundirse unas con otras.

PREFACIO i

INDICE

PROTOCOLOS TCP / IP

CAPITULO 1
DESARROLLO TCP / IP

1.1 INTRODUCCIÓN DE TCP / IP

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un sólo protocolo cuando en realidad son varios, de entre los cuales destaca y es él más importante el protocolo IP.

Para que este protocolo pueda funcionar debe existir comunicación entre los distintos ordenadores conectados a Internet, deben usar el mismo protocolo de comunicaciones y fraccionar la información que se transmite, en los cuales se insertarán las direcciones de los ordenadores origen y destino, asegurándose de que la información transmitida llegue intacta a su destino. Para ello elige las rutas más convenientes hasta el receptor y tras hacer comprobaciones de que la información original quede como inicialmente se envio.

Este protocolo en el momento de enfrentarse con un problema, el sistema que utiliza es dividir el problema en pequeñas porciones hasta que finalmente aborda cada uno de estos problemas y los soluciona.

En 1972 el departamento de defensa de los EEUU solicitó a ARPA(Agencia de Investigación de Proyectos Avanzados) que desarrollará un sistema de red, pero un hubo un problema que las redes que existian utilizaban distintos tipos de sistemas operativos, diversas topologías y tipos de red. Pero como a todo problema hay solución decidieron definir un protocolo(IP)en las redes, en el que más tarde protocolos complejos (TCP, UDP, ICMP, etc.)contribuirían a la solución de problemas en la diversidad de las redes.

1.2 RESEÑA HISTÓRICA DE TCP / IP

- Desarrollado como parte del proyecto DARPA (Agencia de Proyectos de Investigación Avanzada para la Defensa) a mediados de los 70's, dando lugar a la red ARPANET.
- ARPANET utilizaba interconexión de línea rentada punto–punto.
- Su objetivo fue que computadoras cooperativas compartieran recursos mediante una red de comunicaciones.
- En 1980 ARPA comienza a convertir las máquinas conectadas a sus redes con el Protocolo TCP / IP, incluido en la versión 4.2 del UNIX de BERKELEY.
- En 1983 ARPANET se divide en 2 redes separadas: MILNET (Militar) y ARPANET (Investigación).
- 1985 la NSF toma un papel activo para expandir el Internet TCP / IP y comienza un programa para establecer redes de acceso distribuidas alrededor de sus 6 centros de supercomputadoras.

- 1986 NSFNET es una nueva columna vertebral de área amplia que eventualmente alcanzo todos los centros con supercomputadoras y los unió a ARPANET.
- 1991 NSFNET había crecido en un billón de paquetes por día y la capacidad de 1.5 Mbs comenzaba a ser insuficiente.
- 1993 ANS crea una nueva red de columna vertebral que reemplaza a NSFNET y la llama ANSNET la cual opera a 45 Mbs con una capacidad de 30 veces más que NSFNET.

1.3 CARACTERÍSTICAS

- El protocolo TCP/IP es él más utilizado en la INTERNET.
- También se utiliza en redes no-INTERNET.
- Protocolos de no-conexión en el nivel de red.
- Puede funcionar en máquinas de todo tamaño (multiplataforma)
- Conmutación de paquetes entre nodos.
- Protocolos de transporte con funciones de seguridad.
- Las redes se comunican mediante compuertas.

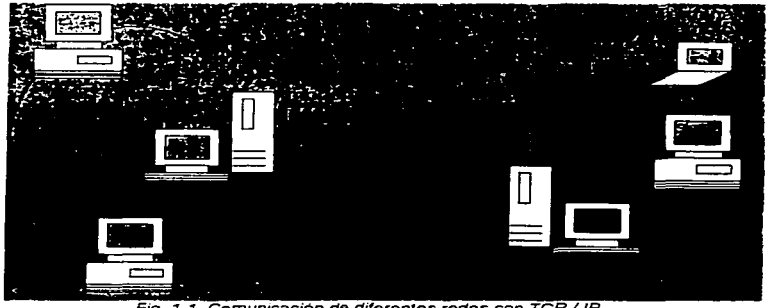


Fig. 1-1 Comunicación de diferentes redes con TCP / IP.

- Todas las redes son vistas como iguales.
- Conjunto común de programas de aplicación.

METAS

- Independencia de tecnología de conexión a bajo nivel y la arquitectura de la computadora.
- Conectividad Universal a través de la red.
- Reconocimientos de extremo a extremo.
- Protocolos de Aplicación Estandarizados.

1.4 ARQUTECTURA DEL PROTOCOLO TCP / IP

Protocolo de control de transmisión / protocolo Internet (**TCP/IP**). El modelo de referencia **TCP/IP** hacen que sea posible la comunicación entre dos computadores (Fig.1-1), desde cualquier parte del mundo, a casi la velocidad de la luz. TCP/IP es compatible con cualquier sistema operativo y tipo de hardware, proporcionando una abstracción total del medio.

El Departamento de Defensa de EE.UU. creó el modelo TCP/IP porque necesitaba una arquitectura que pudiera conectar múltiples redes y que tuviera la capacidad de mantener conexiones aun cuando una parte de la subred esté dañada o perdida.

En la creación de dicho modelo de comunicación estaban implicadas varias universidades americanas, que modificaron el mismo creando un sistema propio, que pasó a llamarse Internetting, que cuando se fue ampliando a redes cada vez mayores se transformó en Internet. Y su base fue el modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló la Red de redes.

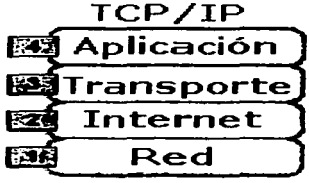


Fig. 1-2 Niveles de aplicación en TCP/IP

El modelo TCP/IP (Fig. 1-2) está basado en el tipo de red Packet-Switched (Conmutación de Paquetes) y tiene cuatro capas: la Capa de Aplicación, la Capa de Transporte, la Capa de Internet y la Capa de Red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI, aunque no se corresponden exactamente unas con otras, por lo que no deben confundirse.

1.4.1 CAPAS DEL PROTOCOLO TCP/IP

CAPA DE APLICACIÓN TCP/IP

Maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por hecho que estos datos están correctamente empaquetados para la siguiente capa.

- FTP: File Transfer Protocol (Protocolo de Transporte de Archivos). Este permite el acceso al sistema de directorios de un ordenador remoto, el envío y la descarga de ficheros de ellos. Como medida de seguridad, el acceso a dichos directorios está protegido por un sistema de control de acceso de tipo Usuario-password.

- TELNET: Protocolo de Servicio de Conexión Remota (Remote Login). Es un emulador de terminal que permite acceder a los recursos y ejecutar programas en un ordenador remoto; es decir, nos permite conectarnos aun equipo remoto y actuar sobre él como si estuviéramos físicamente conectados al mismo.

- HTTP: Hypertext Transfer protocol (Protocolo de Transferencia de Hipertexto). Servicio de páginas web, mediante el cual podemos solicitar éstas a un servidor web y visualizarlas en los navegadores clientes.

- SMTP: Simple Mail Transport Protocol (Protocolo de Transporte de Correo Simple). Servicio de correo electrónico, permitiendo enviar mensajes a otros usuarios de la red. Estos mensajes se envían primero a unos equipos servidores especiales, desde los cuales pueden ser descargados por el destinatario final.

- DNS: Domain Name Service (Servicio de Nombre de Dominio). Servicio de traducción de nombres de domino en direcciones IP reales.

- TFTP: Trival File Transport Protocol (Protocolo de Transporte de Archivo Trivial). El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los diseñadores de software.

CAPA DE TRANSPORTE TCP/IP

Permite que capas pares en los host de fuente y destino puedan conversar. La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Utiliza los servicios de la capa de red para proveer un servicio eficiente y confiable a los procesos de la capa de

aplicación. Realiza una verificación por suma para asegurar que la información no sufrió alteraciones durante su transmisión.

En esta capa se produce la segmentación de los datos producidos en la capa de aplicación en unidades de menor tamaño, denominadas **paquetes** o **datagramas**. Un datagrama es un conjunto de datos que se envía como un mensaje independiente.

La capa de transporte no se preocupa de la ruta que van a seguir los datos para llegar a su destino final. Simplemente considera que la comunicación entre ambos extremos ya está establecida y la utiliza.

En esta aparecen dos protocolos muy importantes:

Protocolo de Datagrama de Usuario (UDP): protocolo no confiable y no orientado a conexión para la entrega de mensajes discretos. En este caso los paquetes enviados mediante el protocolo IP reciben el nombre específico de datagramas, estos se envían y ya está; no se realiza una conexión definida entre los host, ni un control de los paquetes enviados y recibidos. Los datagramas sé rutean independientemente, por lo que deben llevar la dirección completa del destino.

Protocolo para el Control de la Transmisión(TCP): ofrece maneras flexibles de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. Para ello, en el host fuente parte el flujo de bits en mensajes discretos y los envía, mientras que en el host destino los recibe y los monta de nuevo para crear el flujo original, manejando el control de flujo de la transmisión. Las conexiones TCP son punto a punto y full-dúplex, caracterizándose éste último tipo, porque en ellas se permite una transferencia concurrente en ambas direcciones, con lo que en realidad existen dos flujos independientes que se mueven en direcciones opuestas y sin ninguna interacción aparente. Este hace que se reduzca eficazmente el tráfico en la red.

CAPA DE INTERNET O DE RED TCP/IP

El propósito de la capa de Internet es enviar paquetes origen desde cualquier red en Internetwork de redes y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí.

En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Durante su transmisión los paquetes pueden ser divididos en fragmentos, que se montan de nuevo en el destino.

Para poder enrutar los datagramas de la capa de transporte, éstos de encapsulan en unidades independientes, en las que se incorporan diferentes datos necesarios para el envío, como dirección de origen del datagrama, dirección de destino, longitud del mismo, etc.

En una comunicación con arquitectura TCP/IP ambos host pueden introducir paquetes en la red, viajando estos independientemente de cual sea su destino. Por ello, no hay garantía ninguna de entrega de los paquetes ni de orden en los mismos.

En la capa de Internet o red del modelo TCP/IP existe solamente el protocolo de Internet (**IP**) independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento y es la base fundamental de **Internet.**

IP define las unidades de transferencia de datos, denominadas paquetes o datagramas, y se encarga de su transferencia desde el host origen al host destino. Se implementa por software.

IP averigua cómo encaminar los paquetes o datagramas a su destino final, lo que consigue mediante el protocolo IP. Para hacerlo posible, cada interfaz en la red necesita una dirección IP. Una **dirección IP** identifica un host de forma única. Dos host no pueden tener una misma dirección IP pública, pero si pueden tener la misma IP si pertenecen a dos redes privadas diferentes.

El protocolo IP no está orientado a conexión y no es confiable, manda paquetes (datagramas) sin contar con mecanismos de verificación de entrega y sin comprobación de errores. El TCP, se encarga de corregir estas debilidades. En cuanto al ruteo o direccionamiento de los datagramas, se puede realizar paso a paso por todos los nodos o mediante tablas de rutas estáticas o dinámicas.
IP es usado por los de la capa de transporte para encaminar los datos a su destino, siendo ésta su última misión, por lo que no se preocupa de la integridad de la información que contienen los paquetes. Para poder direccionar los datagramas, IP introduce una nueva cabecera en los mismos, normada por 160 bits, que contiene diferentes datos necesarios para poder enrutar los paquetes, como la longitud de la cabecera, la longitud total del datagrama, un número de identificación, tipo de protocolo al que pertenece el datagrama, campo de comprobación (Checksum), dirección de origen, etc.

CAPA DE ACCESO A LA RED TCP/IP

Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN, todos los detalles de las capas física y de enlace de datos del modelo OSI.

Uno de los principales elementos que maneja esta capa es el de las direcciones físicas, números únicos de 6 bytes asignados a cada tarjeta de red y que son el medio principal de localización de un host dentro de una red. Cada tarjeta tiene un número identificador, cuyos 3 primeros bytes son asignados por el fabricante de la misma, mientras que los otros 3 se asignan de forma especial. Cuando un host debe enviar un paquete a otro de su red busca a éste mediante su número de tarjeta de red (dirección física).

Como TCP/IP no especifica claramente un protocolo de nivel de enlace de datos, serán necesarios mecanismos para traducir las direcciones IP a direcciones que entiendan el software de la capa de enlace de datos por sobre el que corre TCP/IP y para controlar posibles errores a nivel de subred. Por eso se introdujeron protocolos específicos, entre los que destacan:

ICMP (Protocolo de Mensajes de Control y Error de Internet): es de características similares a UDP, pero con un formato mucho más simple y su utilidad no está en el transporte de datos de usuario, si no en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Es decir, se usa para manejar mensajes de error y control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

ARP (Protocolo de Resolución de Direcciones): una vez que un paquete llega a una red local mediante el ruteo IP, la entrega del mismo al host destino se debe realizar forzosamente mediante la dirección de Control de Acceso al Medio (MAC) del mismo (número de la tarjeta de red), por lo que hace falta algún mecanismo capaz de transformar la dirección IP que figura como destino en el paquete en la dirección MAC equivalente, es decir, de obtener la relación dirección lógica-dirección física. Esto sucede así porque las direcciones Ethernet y las direcciones IP son dos números distintos que no guardan ninguna relación entre ellos.

El protocolo ARP, en las LAN equipara direcciones IP con direcciones Ethernet (de 48 bits) de forma dinámica. Mediante ARP una máquina determinada (Un router de entrada a la red o un swicht) puede hacer un broadcast mandando un mensaje, denominado petición ARP, a todas las demás máquinas de su red para preguntar qué dirección local pertenece a alguna dirección IP, siendo respondido por la máquina buscada mediante un mensaje de respuesta ARP, en el que le envía su dirección Ethernet. Una vez que la máquina peticionaria tiene este dato envía los paquetes al host destino usando la dirección física obtenida.

RARP (ARP por Réplica): permite que una máquina que acaba de arrancar o sin disco pueda encontrar su dirección IP desde un servidor. Para ello utiliza el direccionamiento físico de red, proporcionando la dirección hardware física (MAC) de la máquina de destino para identificar de manera única el procesador, transmitiendo por difusión la solicitud RARP. Una vez que la máquina obtiene su dirección IP la guarda en memoria, y no vuelve a usar RARP hasta que no se inicia de nuevo.

1.5 MODELO OSI

El Modelo de Referencia de Interconexión de sistemas Abiertos, OSI-RM (Open System Interconection-Reference Model) Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnologías de red utilizados por las empresas a nivel mundial.

ISO dividió el modelo de referencia OSI en capas, entendiéndose por "Capa" una entidad que realiza de por sí una función específica. Cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora(Fig. 1-3), si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

Los criterios que llevaron a este modelo de referencia fueron:

- Deberá crearse una nueva capa siempre que se precise un nuevo grado de abstracción.
- A cada capa deberá asignarse un número bien definido de funciones propias.
- La funcionalidad de cada capa deberá tener en cuenta la posibilidad de definir protocolos normalizados a nivel internacional.
- La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz (especie de pasarela de comunicación entre ellas).
- El número de capas será lo suficientemente grande como para no reunir en un nivel.
- Funcionalidades distintas y lo suficientemente pequeñas para que el resultado final sea manejable en la práctica.

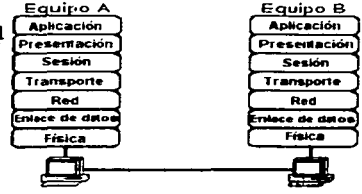


Fig. 1-3 Proceso de comunicación con el modelo OSI

1.6 CARACTERÍSTICAS DEL MODELO OSI

En el modelo de referencia OSI, hay siete capas numeradas (Fig. 1-4) cada una de las cuales ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino.

Las cuatro capas inferiores (Física, Enlace de Datos, Red y Transporte) se encargan de la transmisión de los datos (segmentación, empaquetamiento, enrutamiento, verificación y transmisión por los medios físicos), sin importarles el tipo de datos que se transmiten ni la aplicación que los envía o recibe.

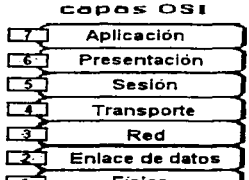


Fig.1-4 Capas en el modelo OSI

Las tres capas superiores (Sesión, Presentación y Aplicación) se encargan del establecimiento de sesiones de comunicación entre aplicaciones, del formateo, cifrado, compresión de datos y de suministrar los mismos a las aplicaciones de usuario de forma adecuada.

1.6.1 PROTOCOLOS

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo.

Un protocolo es un conjunto de normas o convenciones que determinan el formato y la transmisión de datos.

Todo protocolo debe definir los siguientes aspectos en la comunicación de datos:

- Sintaxis: el formato de los datos y los niveles de la señal.
- Semántica: información de control para la coordinación y el manejo de errores.
- Temporización: sincronización de velocidades de secuenciación.

1.6.2 COMUNICACIÓN DE DATOS A TRAVÉS DE REDES

Existen diferentes formas de intercambiar datos a través de una o más redes, entre las que cabe destacar por su importancia:

Conmutación de circuitos: cuando se establece un camino determinado y fijo para intercomunicar dos estaciones a través de los nodos de la red, dedicando en cada enlace un canal lógico a cada conexión. Esto origina que en cada nodo los datos de entrada se encaminen por el canal establecido sin sufrir retardos, transmitiéndose los datos tan rápido como se pueda.

Conmutación de paquetes: donde no es necesario reservar un canal lógico para cada conexión. En cada nodo el paquete de datos entrante se recibe totalmente, se almacena y se transmite al siguiente nodo.

Retransmisión de tramas: surgidas al amparo de las nuevas tecnologías, que permiten una velocidad de transmisión muy elevada con una tasa de errores muy pequeña, lo que hace que no sea necesario adjuntar mucha información de cabecera a cada paquete. Con ello se reduce el tamaño de los paquetes a transmitir, consiguiéndose unas velocidades de transmisión elevadísimas en comparación con el sistema de conmutación de paquetes.

Redes de área local (LAN): de cobertura pequeña y velocidades de transmisión muy elevadas. Utilizan sistemas de difusión (Broadcast) en vez de sistemas de conmutación y no hay nodos intermedios.

Redes de área amplia (WAN): cubren una extensa área geográfica, interconectando generalmente diversas LAN y suelen estar formadas por una serie de dispositivos de

conmutación interconectados. Pueden desarrollarse bien utilizando tecnología de conmutación de circuitos y usando conmutación de paquetes.

ATM: transmite paquetes de tamaño fijo (llamados **Celdas**), ahorrando así información de control en cada trama, con lo que se consigue aumentar notablemente la velocidad de transmisión. En este sistema se dedican canales virtuales de velocidades adaptables a las características de la transmisión (de forma parecida a la conmutación de circuitos).

RDSI y RDSI de banda ancha: sistemas con velocidades de transmisión muy elevadas, basados en conmutación de circuitos (banda estrecha) o en conmutación de paquetes (banda ancha).

1.7 CAPAS DEL MODELO OSI

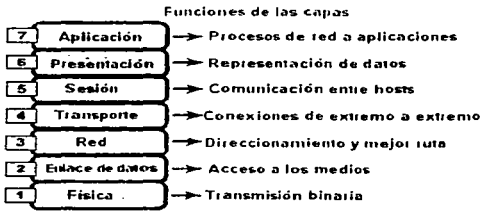


Fig. 1-5 Funciones de las 7 capas del modelo OSI

CAPA DE APLICACIÓN: es la capa del modelo OSI más cercana al usuario, está relacionada con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales. Es el medio por el cual los procesos de aplicación de usuario acceden al entorno OSI.

Su función principal es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones.

Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, estando éstas controladas por protocolos de aplicación y utilizando los servicios del nivel de presentación.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI.

La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí, establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Algunos ejemplos de procesos de aplicación son:

- Programas de hojas de cálculo.
- Programas de procesamiento de texto.
- Transferencia de archivos (FTP).
- Login remoto (RLOGIN, TELNET).
- Correo electrónico (MAIL - SMTP).
- Páginas Web (HTTP).

CAPA DE PRESENTACIÓN: proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo. Su tarea principal es aislar a las capas inferiores del formato de los datos de la aplicación, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red.

Es también la responsable de la obtención y liberalización de la conexión de sesión cuando existen varias alternativas disponibles.

Por ello, de ser necesario, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.

- Definir la estructura de los datos a transmitir. En el caso de un acceso a base de datos, definen el orden de transmisión y la estructura de los registros.

- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).

- Dar formato a la información para visualizarla o imprimirla.

- Comprimir los datos si es necesario.

CAPA DE SESIÓN: proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo, para proceder al intercambio de datos.

PRINCIPALES FUNCIONES

- Establece, administra y finaliza las sesiones entre dos hosts que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, esta capa restaura la sesión a partir de un punto seguro y sin perdida de datos, si esto no es posible termina la sesión de una manera ordenada checando y recuperando todas sus funciones, evitando problemas en sistemas transaccionales.
- Sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos, estableciendo las reglas o protocolos para el diálogo entre máquinas y así poder regular quien habla, por cuanto tiempo o si hablan en forma alterna, es decir, las reglas del diálogo que son acordadas.
- Ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de las Capas de Sesión, Presentación y Aplicación.
- Manejar tokens. Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación.
- Hacer checkpoints, que son puntos de recuerdo en la transferencia de datos.

CAPA DE TRANSPORTE: proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión. Para ello segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor.

PRINCIPALES FUNCIONES

- Controla la interacción entre procesos usuarios.
- Incluye controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Controla el flujo de transacciones y direccionamiento de máquinas a procesos de usuario.
- Asegura que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Acepta los datos del nivel de sesión, fragmentándolos en unidades más pequeñas, llamadas **segmentos**, en caso necesario y los pasa al nivel de red.

- Realiza funciones de control y numeración de unidades de información, fragmentación y reensamblaje de mensajes.

- Se encarga de garantizar la transferencia de información a través de la sub-red.

CAPA DE RED: en esta capa es donde trabajan los routers. Divide los mensajes de la capa de transporte en unidades más complejas, denominadas **paquetes** y los ensambla al final. Debe conocer la topología de la sub-red, manejar el caso en que la fuente y el destino estén en redes distintas.

- Para ello, se encarga de encaminar la información a través de la sub-red, mirando las direcciones del paquete para determinar los métodos de conmutación y enrutamiento, rutea los paquetes de la fuente al destino a través de ruteadores intermedios.

- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.

- Debe controlar la congestión de la sub-red.

CAPA DE ENLACE DE DATOS: proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, formación, entrega ordenada de tramas y control de flujo. Por lo tanto, su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo.

PRINCIPALES FUNCIONES

- Establece los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.

- Agrega una secuencia especial de bits al principio y al final del flujo inicial de bits de los paquetes, estructurando este flujo bajo un formato llamado trama o marco. Suelen ser cientos de bytes.

- Sincroniza el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, envío de acuses de recibo positivos y negativos. Para evitar tramas repetidas se usan números de secuencia en ellas.

- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.

- Controla la congestión de la red.

- Regula la velocidad de tráfico de datos.

- Controla el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción

- Se encarga de la de secuencia, de enlace lógico y acceso al medio (soportes físicos de la red).

CAPA FÍSICA: la misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

PRINCIPALES FUNCIONES

- Definir las características físicas (componentes y conectores mecánicos) y eléctricas (niveles de tensión).

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio. No existe estructura alguna.

- Maneja voltajes y pulsos eléctricos.

- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.

- Garantizar la conexión, pero no la fiabilidad de ésta.

- Esta capa solamente reconoce bits individuales, no reconoce caracteres ni tramas Multicast.

1.7.1 ENCAPSULAMIENTO

Si un computador A desea enviar datos a otro B, en primer término los datos que se deben enviar se deben colocar en paquetes que se puedan administrar y rastrear a través de un proceso denominado encapsulamiento. Las tres capas superiores (Aplicación, Presentación y Sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

Una vez pasados a formato común, el encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al transito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información. La palabra "encabezado" significa que se ha agregado la información correspondiente a la dirección.

Una vez que se envían los datos desde el origen, viajan a través de la capa de aplicación directo hacia las otras capas. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus servicios a los usuarios finales. Como muestra la figura 1-6, las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

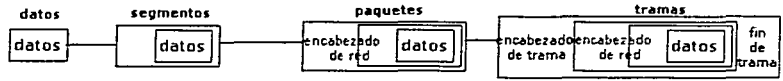


Fig. 1-6 Encapsulamiento que sigue la información para ser enviada a otra máquina.

Crear los datos (Capa de Presentación). Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork.

Empaquetar los datos para ser transportados de extremo a extremo (Capa de Transporte). Se dividen los datos en unidades de un tamaño que se pueda administrar, llamados segmentos y se les asignan números de secuencia para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por la internetwork. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

Agregar la dirección de red al encabezado (Capa de Red). El siguiente proceso se produce en la capa de red, que encapsula el segmento creando un paquete o datagrama, agregándole una dirección de red destino y origen, por lo general IP. Con esto, los datos se colocan en un paquete que contiene el encabezado de red con las direcciones lógicas de origen y destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

Agregar la dirección local al encabezado de enlace de datos (Capa Enlace de datos). En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC de la tarjeta de red, única para cada tarjeta) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

Transmitir el tren de bits creado. (Capa Física). Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, etc.). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física de redes puede variar a lo

largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico puede originarse en una LAN, cruzar el backbone de un campus y salir por un enlace de WAN hasta llegar a su destino en otra LAN remota. Los encabezados y la información final se agregan a medida que los datos se desplazan a través de las capas del modelo OSI.

Cuando los datos se transmiten simplemente en una red de área local, se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a otro host a través de una red interna o Internet, los paquetes se transforman en la unidad de datos a la que se hace referencia. Esto se debe a que la dirección de red del paquete contiene la dirección destino final del host al que se envían los datos (el paquete).

Las tres capas inferiores (Red, Enlace de datos y Física) del Modelo OSI son las capas principales de transporte de los datos a través de una red interna o Internet. La excepción principal a esto es un dispositivo denominado ***gateway***. Este es un dispositivo que ha sido diseñado para convertir los datos desde un formato, creado por las Capas de Aplicación, Presentación y Sesión, en otro formato. De modo que el gateway utiliza las siete capas del modelo OSI para hacer esto.

1.8 COMPARACIÓN OSI - TCP/IP

Si comparamos el modelo OSI y el modelo TCP/IP, observaremos que ambos presentan las siguientes similitudes y diferencias:

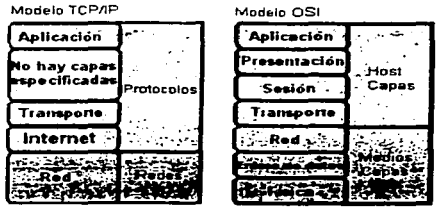


Fig. 1-7 Comparación del Modelo TCP/IP & Modelo OSI

Similitudes:

- Ambos se dividen en capas o niveles.
- Ambos tienen capas de Aplicación, aunque incluyen servicios muy distintos.
- Se supone que la tecnología es de conmutación de paquetes (no de conmutación de circuitos).

- Los profesionales de networking deben conocer ambos: OSI como modelo; TCP/IP como arquitectura real.

Diferencias:

OSI distingue de forma clara los servicios, las interfaces y los protocolos. TCP/IP no lo hace así, no dejando de forma clara esta separación.

- Servicio: lo que una capa hace.
- Interfaz: cómo se pueden acceder a los servicios.
- Protocolo: implementación de los servicios.

- OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente.
- TCP/IP combina las funciones de la Capa de Presentación y Sesión en la Capa de Aplicación.
- TCP/IP combina la Capa de Enlace de Datos y la Capa Física del modelo OSI en una sola capa.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, no se crean redes a partir de protocolos específicos relacionados con OSI, aunque todo el mundo utiliza el modelo OSI como guía.

CAPITULO 2
PROTOCOLOS IP

2.1 PROTOCOLO ICMP

Internet es un sistema autónomo que no dispone de ningún control central. El protocolo ICMP (Internet Control Message Protocol), proporciona el medio para que el software de hosts y gateways intermedios se comuniquen.

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino.

El **Protocolo ICMP** (Protocolo de Mensajes de Control y Error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control (Fig. 2-1).

- El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP.
- El protocolo ICMP tiene su propio número de protocolo (número 1), que lo habilita para utilizar el IP directamente.
- La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP.
- Los mensajes de error de este protocolo los genera y procesa TCP/IP, no el usuario.

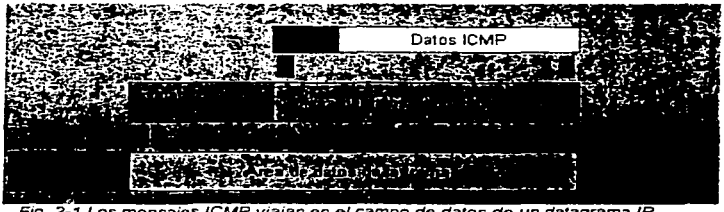


Fig. 2-1 Los mensajes ICMP viajan en el campo de datos de un datagrama IP

- Debido a que el Protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

➢ Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla 2-1; El resto de campos son distintos para cada tipo de mensaje ICMP.

Tipos de mensajes:

Campo de tipo	Tipo de mensaje ICMP
0	Respuesta de eco (Echo Reply)
3	Destino inaccesible (Destination Unreachable)
4	Disminución del tráfico desde el origen (Source Quench)
5	Redireccionar (cambio de ruta) (Redirect)
8	Solicitud de eco (Echo)
11	Tiempo excedido para un datagrama (Time Exceeded)
12	Problema de Parámetros (Parameter Problem)
13	Solicitud de marca de tiempo (Timestamp)
14	Respuesta de marca de tiempo (Timestamp Reply)
15	Solicitud de información (obsoleto) (Information Request)
16	Respuesta de información (obsoleto) (Information Reply)
17	Solicitud de máscara (Addressesmask)
18	Respuesta de la máscara (Addressesmask Reply)

Tabla 2-1 Tipos de mensajes en ICMP

2.1.1 FORMATO DEL MENSAJE ICMP

Cada Mensaje ICMP esta compuesto por los siguientes campos:

- Tipo
- Código
- Checksum
- Otras variables

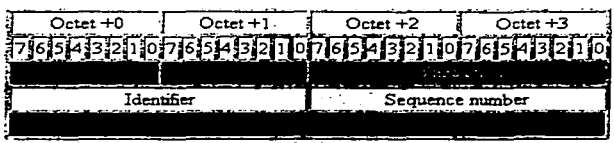


Fig. 2-2 Formato de mensajes en ICMP

El formato de ICMP cambia dependiendo de la función que se realice, exceptuando los campos de Tipo, Código y Checksum. Un 1 en el campo de protocolo del mensaje IP indicará que se trata de un datagrama ICMP.

- La función de un mensaje determinado ICMP estará definida por el campo de Tipo.
- El Código proporciona información adicional para realizar la función.
- El Checksum sirve para efectuar una verificación por suma que sólo corresponde al mensaje ICMP.

2.2 PROTOCOLO IGMP

- El IGMP (Internet Group Management Protocol) es un protocolo que funciona como una extensión del protocolo IP.
- Se utiliza exclusivamente por los miembros de una red multicast para mantener su status de miembros, o para propagar información de direccionamiento.
- Un gateway multicast manda mensajes una vez por minuto como máximo. Un host receptor responde con un mensaje IGMP, que marca al host como miembro activo. Un host que no responde al mensaje se marca como inactivo en las tablas de direccionamiento de la red multicast.

2.3 PROTOCOLO ARP

ARP ***(Address Resolution Protocol)***

Es el protocolo encargado de asociar direcciones de red con direcciones físicas. Para que dos estaciones de una red local puedan comunicarse, es necesario realizar esta asociación, ya que serán las direcciones físicas de las tarjetas de red las que permitan identificar en último termino una estación de la red local.

Las implementaciones del protocolo ARP incorporan buffers con las tablas de correspondencia entre direcciones IP y direcciones físicas de la red, de forma que se reduce el número de consultas que se deben realizar.

ARP fue diseñado en su origen para redes *Ethernet*, pero se puede hacer uso de él en otros tipos de redes como *Arcnet*, *Token Ring* o Redes de Fibra óptica.

Fundamentalmente se divide en dos partes:

- Primero envía un *broadcast* para localizar la dirección física, asignada a la dirección IP.
- La segunda es la respuesta de la máquina a la cual corresponde la dirección física.

2.3.1 FORMATO DEL MENSAJE ARP

El mensaje ARP esta formado por 28 octetos. En los campos que se describen a continuación se supone un Interfaz Ethernet.

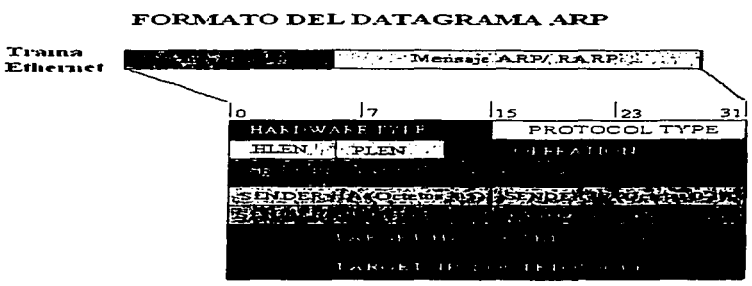


Fig. 2-3 Formato de un datagrama ARP para una trama de red Ethernet

Tipo de Hardware

El campo Hardware (Tabla 2-2) indica el tipo de interfaz de Hardware. Por Ejemplo, el valor de una red Ethernet es 1.

Tabla 2-2 Tipo de hardware

Tipo de Interfaz de Hardware

Tipo	Descripción
1	Ethernet (10mb)
2	Experimental Ethernet (3 mb)
3	Amateur Radio X.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Network
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNET or Sytek Inc. Localnet)

Números de Protocolo (PROTOCOL TYPE)
El campo protocolo identifica el protocolo Ethernet usado. Por ejemplo el valor del interfaz Ethernet es 0800 hex.

Longitud de la dirección Hardware (HLENG)
El valor para Ethernet es 6, lo que proporciona 48 bits para una dirección Ethernet (12 semi-octetos).

Longitud del Protocolo (PLEN)
Este campo se usa para definir la longitud de la dirección de red. Indica el número de octetos de las direcciones de las capas de red. Normalmente IP es 4.

Operación (OPERATION)
Especifica el código de la operación. La solicitud ARP (REQUEST) tiene valor 1 y la respuesta ARP(RESPONSE) tiene valor 2.

Dirección Hardware del Origen(ADDRESSES)
Los campos dirección hardware del origen, dirección IP del origen y dirección IP del destino los completa el emisor (si los conoce). El receptor añade la dirección hardware del destino y devuelve el mensaje al emisor con el código de operación 2. (El código de la Respuesta ARP).

La dirección hardware de origen (para Ethernet) esta formada por octetos que representan una dirección Ethernet de 48 bits, o un número.

Dirección IP de Origen
La dirección IP de origen puede ser una dirección de clase A, B o C. (Direcciones IP para obtener una definición de estas clases).

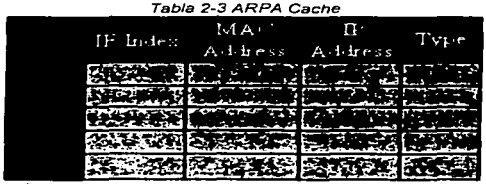
Dirección Hardware de Destino
Este campo esta formado igual que el campo dirección hardware de origen.

Dirección IP de Destino
Este campo es igual que el campo dirección IP de origen.

2.3.2 ARP CACHE

Básicamente, el ARP es una lista de direcciones IP y sus respectivas direcciones físicas. Está Tabla 2-3 se le conoce como **ARP cache**.

Tabla 2-3 ARPA Cache



Cada renglón de la tabla corresponde a un dispositivo.

Antes de efectuarse un Request ARP busca en el ARP cache, en caso de encontrar la dirección MAC realiza el Request. Una vez que se obtiene la dirección se agrega a la tabla.

2.3.3 PROCESO ARP

- La interfase de red recibe un datagrama IP a enviar (Request) a un equipo destino, en este nivel se coteja la tabla temporal de conversión, si existe una referencia adecuada ésta se incorpora al paquete y se envía.

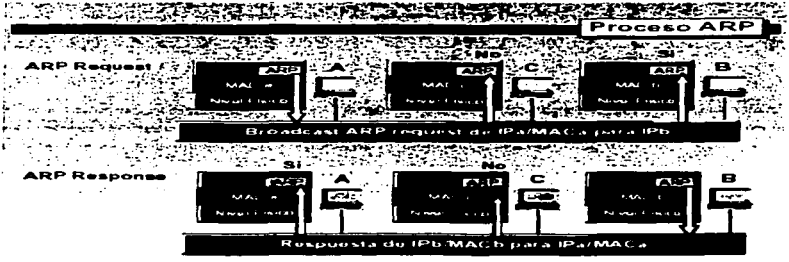


Fig. 2-4 Proceso ARP una máquina origen envía un mensaje en la red con una dirección IP, todas las reciben el mensaje y comparan la dirección IP con la propia y envían una respuesta.

- Si no existe la referencia de un paquete ARP de emisión general, con la dirección IP de destino, es generado y enviado.

- Todos los equipos en la red física reciben el mensaje general y comparan la dirección IP que contiene con la suya propia, enviando un paquete de respuesta(Response)que contiene su dirección IP.

- La computadora origen actualiza su tabla temporal y envía el paquete IP original y los subsecuentes, directamente a la computadora destino.

2.4 PROTOCOLO RARP

Una variante de **ARP** es **RARP** *(Reverse ARP)*. Su función es permitir a una estación de una red obtener su dirección IP conociendo únicamente su dirección física. Esta estrategia se suele utilizar para que las estaciones de red sin disco obtengan su configuración desde un servidor de red.

Una estación que utilice el protocolo **RARP** envía un mensaje a toda la red *(broadcast)* indicando su dirección física y solicitando su dirección **IP**. Un servidor de la red que actúe como servidor de direcciones y este en disposición de ofrecer tal información, leerá la solicitud y consultara su tabla **RARP** para ver que dirección **IP** corresponde a la dirección MAC indicada en la petición, devolviendo dicha dirección.

2.4.1 FORMATO DEL MENSAJE RARP

El formato del RARP es similar al del ARP. El valor del código de operación para una solicitud (Request) es 3, y el valor para una respuesta(Response) es 4.

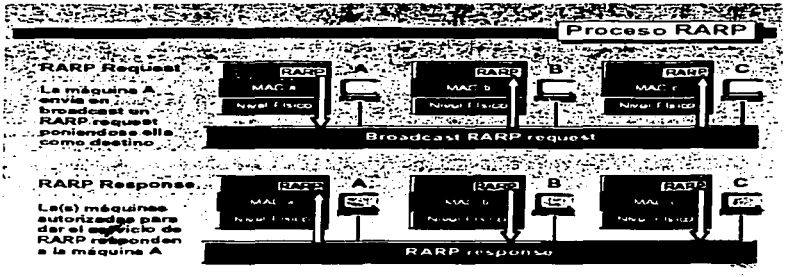


Fig. 2-5 Proceso del mensaje RARP

2.5 PROTOCOLO IP

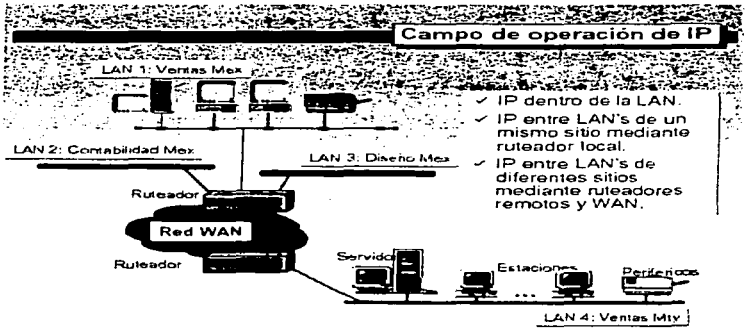


Fig. 2-6 Campo de operacion del protocolo internet

IP (Internet Protocol)

El Protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base sólida. El protocolo IP especifica que la unidad básica transferencia de datos en el TCP/IP es el datagrama.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentados intencionadamente para permitir que un nodo con un buffer limitado pueda recoger todo el datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos de datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la máquina origen (Esto lo hace el protocolo ICMP).

El Protocolo IP también define cual será la ruta inicial por la que serán mandados los datos.

Cuando los datagramas viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Maximum Transmission Unit) y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU. El datagrama consiste en una cabecera y datos.

2.5.1 CARACTERÍSTICAS DE IP

- Protocolo orientado a no-conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones lógicas IP de 32 bits.
- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.
- Realiza él "mejor esfuerzo" para la distribución de paquetes.
- Tamaño máximo del paquete de 65635 bytes.
- Sólo se realiza verificación por suma al encabezado del paquete, no a los datos éste que contiene.

2.5.2 FUNCIONES BASICAS DE IP

IP implementa dos funciones básicas: el encaminamiento y la fragmentación. Para la primera de las funciones se sirve de uno de los campos que aparecen en la cabecera de los datagramas, se trata de la dirección IP del host destino. Esta dirección es utilizada para transmitir los datagramas hacia el host correspondiente.
La segunda de las funciones esta influenciada por el nivel que se encuentra situado justo debajo de la capa IP, se trata del nivel de enlace. Los datagramas generados por IP deben amoldarse al tamaño máximo que es capaz de tratar la red, el cual esta limitado por la capa del nivel de enlace. Si el tamaño máximo de una trama (nombre que recibe la unidad de datos a nivel de enlace) es menor que el datagrama generado por IP, entonces la capa IP se ve obligada a fragmentar, de manera que los datagramas resultantes pueden ser enviados por la red.

El protocolo IP trata cada datagrama como una unidad independiente del resto de los datagramas, no existen conexiones, ni circuitos virtuales en él envió de la información. Para llevar a cabo su servicio, IP utiliza cuatro campos especiales llamados:

*Tipo de servicio

*Tiempo de vida

*Opciones

*Checksum

- El tipo de servicio indica la calidad del servicio deseada.

- El tiempo de vida establece el tiempo máximo que un datagrama puede tardar en alcanzar su destino. Este tiempo se va decrementando a medida que el datagrama atraviesa los diferentes nodos de la red. Cuando el valor de este campo llega a cero, el datagrama se descarta.

- Las opciones proporcionan funcionalidad de control en algunas situaciones, se incluyen entre otros, mecanismos de seguridad, encaminamiento especial, etc.

- El campo *checksum* proporciona la verificación de que la información se ha recibido de manera correcta; sin embargo, esta comprobación se hace únicamente a nivel de la cabecera; por lo que no existe garantía de que la información que transporta el datagrama sea correcta. Si el checksum falla el datagrama se descarta.

2.6 DATAGRAMA IP

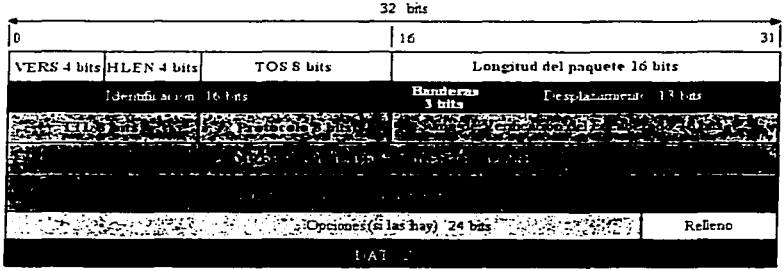
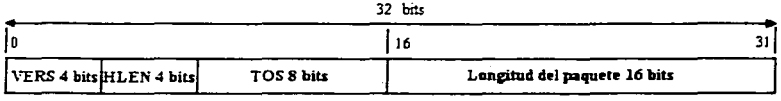


Fig. 2-7 Formato del datagrama del protocolo IP

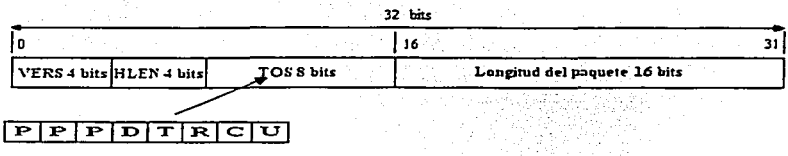


Longitud de la Cabecera (HLEN)
Este campo ocupa 4 bits y representa el número de octetos de la cabecera dividido por cuatro, lo que hace que este sea el número de grupos de 4 octetos (32 bits) en la cabecera.

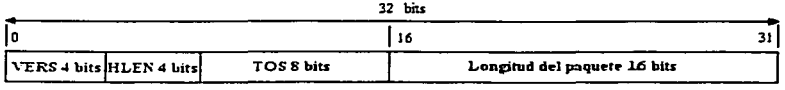
Versión (VERS)
El campo versión ocupa 4 bits. Este campo hace que diferentes versiones del protocolo IP puedan operar en la Internet. La versión actual es 4 y en un futuro será la versión 6 ó IPng.

Tipo de servicio (TOS)
Este campo ocupa un octeto de la cabecera IP, especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican la precedencia. Los valores de la precedencia pueden ser de 0 a 7. Cero es la precedencia normal, 7 esta reservado para control de red. Muchos gateways ignoran este campo.

Los otros 4 bits definen el campo prioridad, que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0 (por defecto, servicio normal), 1 (minimizar el costo monetario), 2 (máxima fiabilidad), 4 (maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los routers para direccionar las solicitudes de los usuarios.



P : Estos 3 bits indican uno de los 8 niveles posibles de procedencia o prioridad.
D: Solicita una conexión de bajo retardo. Retraso normal si vale 0 y retraso bajo si vale 1.
T: Indica rendimiento normal si vale 0 y rendimiento elevado si vale 1.
R: Solicita alta confiabilidad. Si vale 0 fiabilidad normal y si vale 1 fiabilidad alta.
C: Solicita una ruta con más bajo costo.
U: No se usa.



Longitud Total
Este campo se utiliza para identificar el número de octetos en el datagrama total. El paquete consta de 16 bits y es la longitud total del datagrama de IP medido en octetos incluyendo el encabezado y los datos. Los 16 bits de este campo significan que el tamaño máximo del datagrama es de 65535 octetos.

Identificación
El valor del campo identificación es un número secuencial asignado por el host origen. El campo ocupa dos octetos. Los números oscilan entre 0 y 65535, que cuando se

combinan con la dirección del host forman un número único en la Internet. El número se usa para ayudar en el reensamblaje de los fragmentos de datagramas.

Flags

El campo flag ocupa 3 bits y contiene dos flags. El bit 5 del campo flags se utiliza para indicar el último datagrama fragmentado cuando toma valor cero. El bit 7 lo utiliza el servidor origen para evitar la fragmentación. Cuando este bit toma valor diferente de cero y la longitud de un datagrama excede el MTU, el datagrama es descartado y un mensaje de error es enviado al host de origen por medio del protocolo ICMP.

Desplazamiento de los fragmentos

Cuando el tamaño de un datagrama excede el MTU, este se segmenta.
El desplazamiento del fragmento consta de 13 bits y este campo es utilizado con los datagramas fragmentados para indicar la posición, donde los datos de este fragmento ocupan el inicio del datagrama entero.

Tiempo de Vida(TTL)

El campo tiempo de vida ocupa un octeto. Representa el número máximo de segundos que un datagrama puede existir en Internet, antes de ser descartado. Un Datagrama puede existir un máximo de 255 segundos. El número recomendado para IP es 64. Se ajusta a un valor inicial que se va decrementando en cada ruteador.
El originador del datagrama manda un mensaje ICMP, cuando el datagrama es descartado.

Protocolo

El campo protocolo se utiliza para identificar la capa de mayor nivel más cercana usando el IP. Este es un campo de 0 bits, que normalmente identifica tanto la capa TCP (valor 6), como la capa UDP (valor 17) en el nivel de transporte, pero puede identificar hasta 255 protocolos de la capa de transporte.

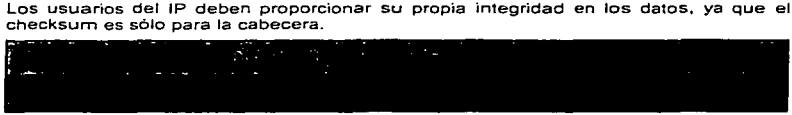
Suma de verificación(Checksum)

El checksum proporciona la seguridad de que el datagrama no ha sido dañado ni modificado. Este campo tiene una longitud de 16 bits.

El checksum incluye todos los campos de todos los campos de la cabecera IP, incluido el mismo, cuyo valor es cero a efectos de cálculo.

Un gateway o nodo que efectúe alguna modificación en los campos de la cabecera (por ejemplo en el tiempo de vida), debe recalcular el valor del checksum antes de enviar el datagrama.

Los usuarios del IP deben proporcionar su propia integridad en los datos, ya que el checksum es sólo para la cabecera.



Dirección de Origen(SOURCE ADDRESS)
Este campo contiene un identificador de red (Netid) y un identificador de host (Hostid). El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C.

Dirección de Destino(DESTINATION ADDRESS)
Este campo contiene el Netid y el Hostid del destino. El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C o D.

Opciones(si las hay) 24 bits	Relleno

Opciones (OPTIONS)
La existencia de este campo viene determinada por la longitud de la cabecera. Si esta es mayor de cinco, por lo menos existe una opción.

Aunque un host no esta obligado a poner opciones, puede aceptar y procesar opciones recibidas en un datagrama. El campo opciones es de longitud variable. Cada octeto esta formado por los campos copia, clase de opción y número de opción. Soporta facilidades de un debug(supresor de errores) mediciones y seguridad.

- El campo copia sirve para que cuando un datagrama va a ser fragmentado y viaja a través de nodos o gateways. Cuando tiene valor 1, las opciones son las mismas para todos los fragmentos, pero si toma valor 0, las opciones son eliminadas.

- Clase de opción es un campo que cuando tiene valor 0, indica datagrama o control de red; cuando tiene valor 2, indica depuración o medida. Los valores 1 y 3 están reservados para un uso futuro.

- El Número de opción indica una acción especifica.

Relleno (PADDING)
Cuando esta presente el *campo pad*, consiste en 1 a 3 octetos puestos a cero, si es necesario, para hacer que el número total de octetos en la cabecera sea divisible por cuatro y así conformar la palabra que puede ser el punto correcto del inicio de los datos cuando las opciones de longitud de variables están presentes.

DATOS

Datos

- El campo datos consiste en una cadena de octetos. Cada octeto tiene un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo, dependiendo del medio físico. El tamaño máximo esta definido por la longitud total del datagrama.
- Es variable e incluye los encabezados de los protocolos de niveles superiores y los datos del usuario.
- Dado que el encabezado de longitud total es de 16 bits, el tamaño máximo del datagrama es de 65535 octetos.
- Tanto los ruteadores como los host manejan datagramas como un mínimo de 576 bytes.

2.7 DIRECCIONES IP

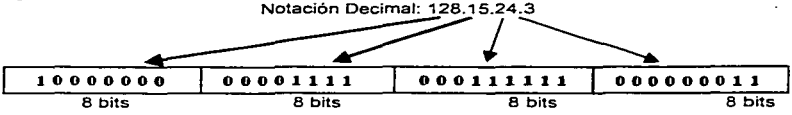
Las direcciones IP hacen que él envió de datos entre ordenadores se haga de forma eficaz.

Las direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits separados por puntos. Con lo cual se tiene la posibilidad de manejar 4,294,967,296 direcciones diferentes.
Identifica a las redes y a los nodos conectados a ellas. Especifica la conexión entre redes.

Se representan mediante cuatro octetos, escritos en formato decimal, separados por puntos.

Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Las direcciones se escriben en un formato decimal como se muestra en la siguiente figura:



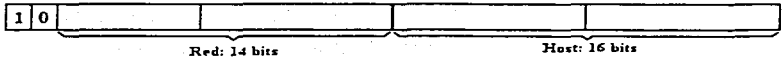
Clases de Direcciones IP

Estas se clasifican en 5 clases diferentes:

Clase A

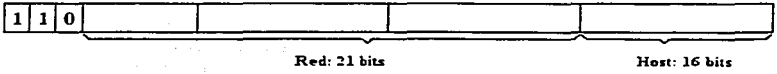
La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes con 16,777,216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0 y 127.255.255.255 , la máscara de subred será 255.0.0.0

Clase B



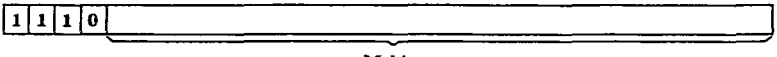
La clase B contiene 14 bits para direcciones de red y 16 bits para direcciones de hosts. El número máximo de redes es 16,536 redes con 65,536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0 y 191.255.255.255, la máscara de subred será 255.255.0.0

Clase C



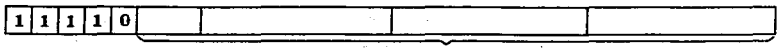
La clase C contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2,097,142 redes, cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0 y 223.255.255.255, la máscara de subred será 255.255.255

Clase D



La clase D se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0 y 239.255.255.255

Clase E

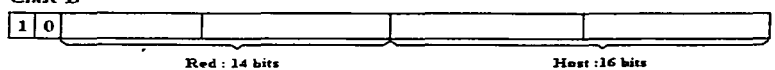


La clase E se utiliza exclusivamente para fines experimentales. Las direcciones están comprendidas entre 240.0.0.0 y 247.255.255.255

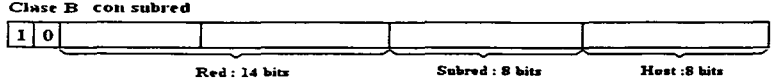
2.8 SUBREDES

- Las Subredes son redes físicas distintas que comparten una misma dirección IP.
- Deben identificarse una de otra usando una máscara de subred.
- La máscara de subred es de cuatro bytes y para obtener el número de subred se realiza una operación AND lógica entre ella y la dirección IP de algún equipo.
- La máscara de subred deberá ser la misma para todos los equipos de la red IP.
- Las distintas clases de direcciones IP pueden ser divididas en unidades más pequeñas con el fin de brindar mayor flexibilidad al administrador de la red.
- A continuación un ejemplo en donde una dirección Clase B es dividida en subredes tomando 8 bits de los correspondientes al host.

Clase B



Clase B con subred



2.9 MÁSCARA DE RED IP

Cuando dos o más redes diferentes se encuentran conectadas entre sí por medio de un router, éste debe disponer de algún medio para diferenciar los paquetes que van dirigidos a los host de cada una de las redes. Es aquí donde entra en juego el concepto de máscara de red, que es una especie de dirección IP especial que permite efectuar este enrutamiento interno de paquetes (Fig. 2-8).

Dada una dirección IP de red cualquiera, la máscara de red asociada es aquella que en binario tiene todos los bits que definen la red puestos a 1 (255 en decimal) y los bits correspondientes a los host puestos a 0 (0 en decimal). Así, las máscaras de red de los diferentes tipos de redes son:

Red Clase A.....Máscara de red =255.0.0.0

Red Clase B.....Máscara de red =255.255.0.0

Red Clase C.....Máscara de red =255.255.255.0

La máscara de red posee la importante propiedad de que cuando se combina con la dirección IP de un host se obtiene la dirección propia de la red en la que se encuentra el mismo. Cuando al router que conecta varias redes le llega un paquete saca de él la dirección IP del host destino y realiza una operación AND lógica entre ésta IP y las diferentes máscaras de red de las redes que une, comprobando si el resultado coincide con alguna de las direcciones propias de red. Este proceso de identificación de la red destino de un paquete (host al que va dirigido el paquete) se denomina enrutamiento.

Los routers poseen unas tablas de enrutamiento en las que almacenan información sobre el mejor camino que pueden seguir los paquetes para llegar a su destino. Cuando le llegan los paquetes el router debe extraer de ellos la dirección de la red a la que pertenecen, para saber a cuál de las redes que une deben mandar los paquetes. Para ello, escoge la dirección IP de destino y realiza con ella y las máscaras de red de cada una de las redes a las que pertenece una operación AND lógica, con lo que obtendrá la dirección de la red destino. Para realizar la operación AND pasa las direcciones IP a formato binario:

host : 220.2.110.10 = 11011100.00000010.01101110.00001010

Máscara de red: 255.255.255.0 = 11111111.11111111.11111111.00000000

Resultado de operación AND: 11011100.00000010.01101110.0000000000 = 220.2.110.0

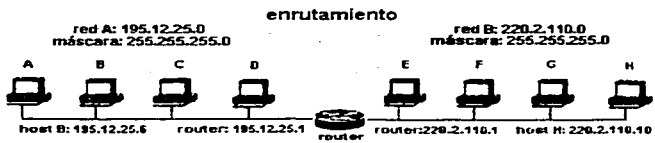


Fig. 2-8 Enrutamineto de paquetes en una red

Con esto, el router sabe que debe enviar los paquetes a la red B, de dirección de red 220.2.110.0 Entonces, actuando como un host más de la misma, consulta su tabla de resolución ARP, obtiene la dirección de tarjeta y le envía directamente los paquetes.

2.10 FRAGMENTACION Y REENSAMBLAJE

- Esto puede suceder en el área LAN-WAN y LAN-LAN (Fig. 2-9).
- La fragmentación (Fig. 2-10) en un datagrama IP es necesaria cuando el tamaño de dicho datagrama excede el tamaño máximo permitido para atravesar una red y poder alcanzar su destino.
- El tamaño de los datagramas está sujeto a la máxima capacidad de las tramas del nivel 2 e IP se encarga de reducirlo(fragmentar).

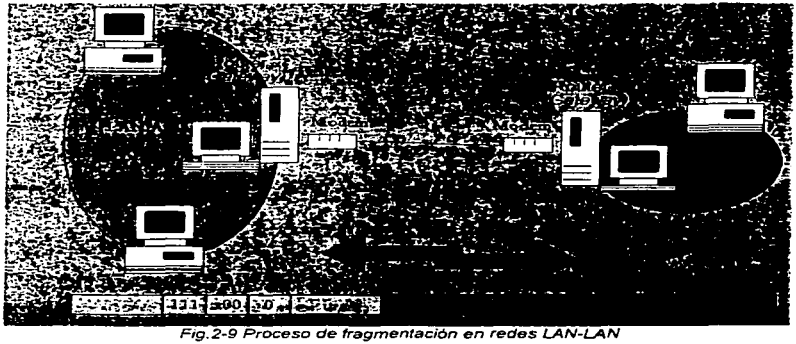


Fig.2-9 Proceso de fragmentación en redes LAN-LAN

- En un principio los niveles superiores pueden entregar a IP paquetes de información de cualquier tamaño e IP se debe encargar de fragmentar y reensamblar cuando se excede la capacidad de las tramas del nivel 2.
- Al límite del nivel 2 visto por IP se le conoce como MTU(Maximum Transfer Unit).
- Un datagrama puede estar marcado para que no pueda fragmentarse, en tal caso, al llegar a un punto en el que la fragmentación sea inevitable, dicho datagrama se descartaría, enviando un mensaje ICMP al emisor del datagrama.

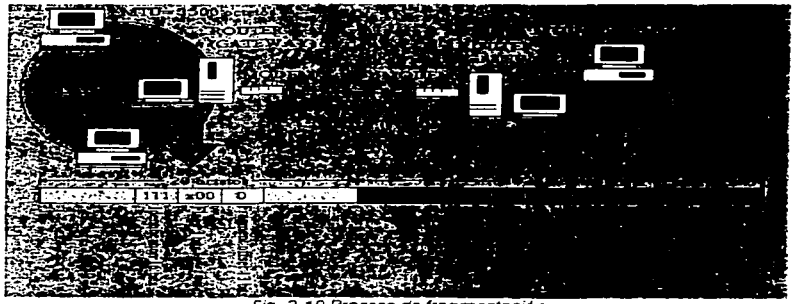


Fig. 2-10 Proceso de fragmentación

- Todos los fragmentos transportan los 32 bits que identifican a todos los fragmentos de un mismo datagrama, si es el último fragmento del datagrama y la posición del fragmento dentro del datagrama.

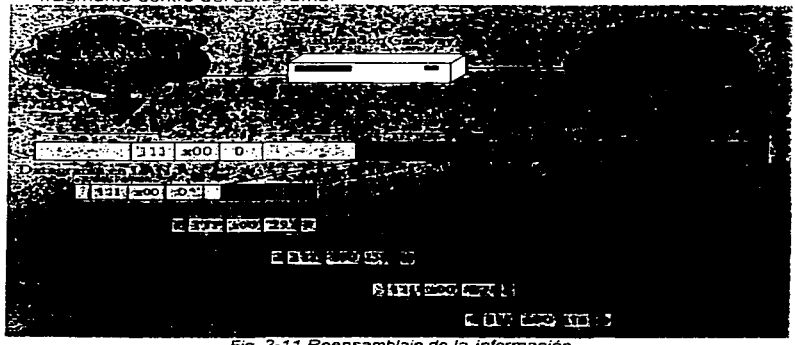


Fig. 2-11 Reensamblaje de la información

- Con esta información es posible realizar el reensamblaje(Fig. 2-11), el cual sólo se realiza en el destino final.

CAPITULO 3
PROTOCOLOS TCP

3.1 PROTOCOLO TCP

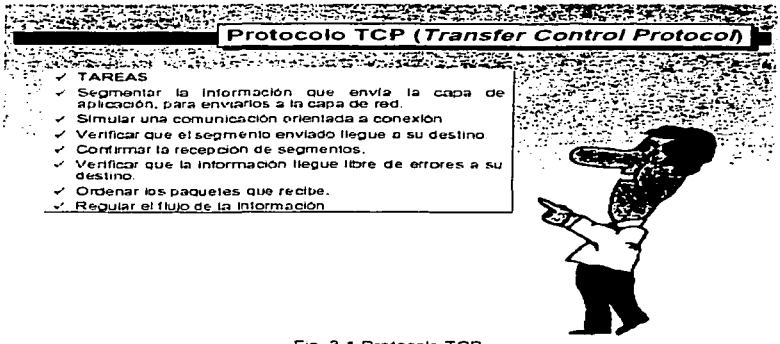


Fig. 3-1 Protocolo TCP

PROTOCOLO TCP

El Protocolo de Control de Transmisión (TCP) es el método más eficiente y seguro de mover trafico de red entre un cliente y un servidor o entre subredes en general. Aunque TCP se presenta como parte del grupo de protocolos de Internet (TCP/IP), es un protocolo de propósito general que se puede adaptar para utilizarlo con otros sistemas de entrega.

TCP es un protocolo orientado a conexión que genera un circuito virtual entre dos entidades de red y que proporciona fiabilidad extremo a extremo. Para garantizar el buen funcionamiento de la red, TCP utiliza diferentes técnicas que maximizan el rendimiento de las conexiones, asegurando que los segmentos de datos que manipula tienen un tamaño óptimo y la velocidad de envío es la más indicada para el circuito virtual establecido. TCP utiliza una técnica conocida como ***acuse de recibo*** para garantizar la llegada de los datos a la entidad remota.

3.1.1 CARACTERÍSTICAS TCP

- Proporciona comunicación bidireccional completa mediante circuitos virtuales.
- Desde el punto de vista del usuario la información es transmitida por flujos de datos.
- Confiabilidad en la transmisión de datos por medio de:

1. Asignación de números de secuencia a la información segmentada.

2. Validaciones por suma.
3. Reconocimiento de paquetes recibidos.
4. Utiliza el principio de ventana deslizable para esperar reconocimientos y reenviar información.

❖ **Fiabilidad en la transferencia de TCP**
Cada vez que un paquete es enviado sé inicializa un contador de tiempo, al alcanzar el tiempo de expiración, sin haber recibido el reconocimiento, el paquete se reenvía. Al llegar el reconocimiento el tiempo de expiración se cancela.

❖ **Protocolo Orientado a Conexión**
Las aplicaciones solicitan la conexión al destino, luego usan esta conexión para entregar y transferir los datos, garantizando que estos serán entregados sin problemas.

❖ **Punto a Punto**
Una conexión TCP tiene dos extremos, que son los entes que participan en la comunicación, es decir, emisor y receptor.

❖ **Confiabilidad**
TCP garantiza que los datos transferidos serán entregados sin ninguna pérdida, duplicación o errores de transmisión.

❖ **Full Dúplex**
Los extremos que participan en una conexión TCP pueden intercambiar datos en ambas direcciones simultáneamente

❖ **Conexión de Inicio Confiable**
El uso del three-way handshake garantiza una condición de inicio confiable y sincronizada entre los extremos de la conexión.

❖ **Término de Conexión Aceptable.**
TCP garantiza la entrega de todos los datos antes de la finalización de la conexión.

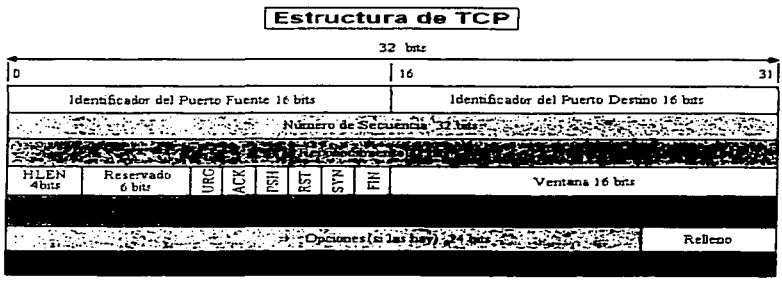
Debido a que TCP, al igual que UDP, están en la capa de transporte, necesita valerse de IP para el envío de sus segmentos o mensajes. De esta manera, IP trata al mensaje TCP como la información que debe entregar y en ningún momento intenta interpretar su contenido, como generalmente se hace al pasar un mensaje de una capa a otra inferior.

Los extremos de la conexión son identificados por puertos, lo que garantiza que se puedan establecer múltiples conexiones en cada host y que los puertos puedan estar asociados con una aplicación o un puerto directamente. De lo anterior se desprende que los routers o cualquier dispositivo de nivel tres sólo puede observar los encabezados IP (nivel de red) para el reenvío de los datagramas, nunca interpretarán los datos de un nivel superior, pues esto supone violar el modelo de capas. Por lo tanto,

TCP en la máquina destino, es el encargado de interpretar los mensajes TCP, después de recibirlos de la capa de red, quien previamente le ha quitado el encabezado IP.

TCP usa diversas técnicas para proveer la entrega confiable de datos. Estas técnicas permiten a TCP recobrarse de errores como paquetes perdidos, duplicados, retardo, diferentes velocidades de transmisión entre nodos y congestión.

3.2 ESTRUCTURA DE TCP



HLEN Header lenght
ACK Acknowledgement
RST Reset the connection
URG Urgent
PSH Push request
SYN Synchronize
FIN Final flag, connection terminated

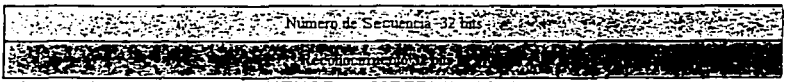
Fig. 3-2 Formato del Protocolo TCP

Descripción de los campos TCP

Identificador del Puerto Fuente 16 bits	Identificador del Puerto Destino 16 bits

Puerto fuente (SOURCE PORT)
Campo de 16 bits. Que identifica el puerto de la máquina origen. Al igual que el puerto destino es necesario para identificar la conexión actual.

Puerto destino (DESTINATION PORT)
Campo de 16 bits. Puerto de la máquina destino.



Número de secuencia (SEQUENCE NUMBER) (32 bits)
Indica el número de secuencia del primer byte que trasporta el segmento.

Número de acuse de recibo(ACKNOWLEDGEMENT NUMBER)(32 bits).
Indica el número de secuencia del siguiente byte que se espera recibir. Con este campo se indica al otro extremo de la conexión que los bytes anteriores se han recibido correctamente.

HLEN 4bits	Reservado 6 bits

HLEN (4 bits). Longitud de la cabecera medida en múltiplos de 32 bits (4 bytes). El valor mínimo de este campo es 5, que corresponde a un segmento sin datos (20 bytes).

Reservado (6 bits). Bits reservados para un posible uso futuro.

Bits de código o indicadores (6 bits). Los bits de código determinan el propósito y contenido del segmento. A continuación se explica el significado de cada uno de estos bits (mostrados de izquierda a derecha) si está a 1.

URG	ACK	PSH	RST	SYN	FIN

URG: indica que el segmento transporta datos urgentes, el campo puntero de urgencia contiene información válida.

ACK: el campo número de acuse de recibo contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación. Debido a que los datagramas no se van recibiendo en orden, únicamente se podrán confirmar aquellos segmentos que se hayan recibido.

PSH: la aplicación ha solicitado una operación push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento). Indica que los datos que transporta el segmento TCP deben ser enviados a la aplicación lo antes posible.

RST: indica que la conexión debe ser reiniciada.

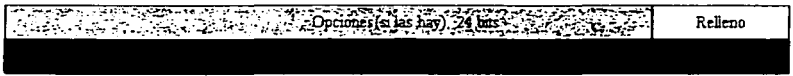
SYN: sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir.

FIN: indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual al host.

Ventana (16 bits). Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino. Puede variarse en cualquier momento mientras la conexión este activa.

Suma de verificación(CHECKSUM): Tiene un tamaño de 2 bytes. Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Se calcula tomando él complementó a uno de 16 bits de la suma de complementos a uno de las palabras de 16 bits en el encabezado (incluyendo el pseudo-encabezado) y el texto juntos.

Puntero de urgencia (8 bits). Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte del campo datos que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes. Nótese que un mismo segmento puede contener tanto datos urgentes (al principio) como normales (después de los urgentes).



Opciones (variable): si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.

Relleno(PADDING): se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.

Datos: información que envía la aplicación. Es variable e incluye los encabezados de los protocolos de niveles superiores y en algunas ocasiones los datos del usuario.

3.3 FUNCIONAMIENTO DEL PROTOCOLO TCP

Fig. 3-3 Funcionamiento TCP

- Antes de enviarle información para su ruteamiento, TCP establece un circuito virtual para garantizar la comunicación en los dos sentidos.
- Tanto la solicitud como el acuse incluyen un número de socket que identifica la conexión tanto de la máquina emisora como en la receptora.
- El socket es un número único y se compone de la dirección IP y el número de puerto TCP al que se conectan.

3.4 PROTOCOLO UDP

UDP *User Datagram Protocol* (Protocolo de Datagrama de Usuario) proporciona el mecanismo primario que utilizan los programas del nivel de aplicación para enviar datagramas a otros programas del mismo nivel.

UDP es un protocolo no orientado a conexión, que transporta un flujo de bytes, conocido como *datagrama*, desde una máquina origen basta otra máquina destino. UDP no es un protocolo fiable, debido a que no garantiza la llegada de los mensajes ni la retransmisión de los mismos.

Un programa de aplicación que utiliza UDP acepta toda la responsabilidad sobre la pérdida, duplicación, retraso de los mensajes, la entrega fuera de orden, etc. Si la aplicación incluye un identificador con su mensaje de petición, el servidor puede reconocer los datagramas duplicados y llevar a cabo el descarte de los mismos, sin embargo, este mecanismo es labor del programa de aplicación y no del protocolo UDP. Por esto UDP suele utilizarse en redes de área local(LAN) donde las redes son fiables y no es necesario un control riguroso del trafico de datos.

Este protocolo deja al programa de aplicación a ser explotado, la responsabilidad de una transmisión fiable. Con él puede darse el caso de que los paquetes se pierdan o bien no sean reconstruidos en forma adecuada. Permite un intercambio de datagramas más directo entre aplicaciones y puede elegirse para aquellas que no demanden una gran cantidad de datagramas para operar óptimamente.

3.4.1 CARACTERISTICAS UDP

- Proporciona de mecanismos primordiales para que programas de aplicación se comuniquen con otros en computadoras remotas.
- Utiliza el concepto de puerto para permitir que múltiples conexiones accedan a un programa de aplicación.
- Provee un servicio no confiable orientado a no-conexión.
- El programa de aplicación tiene la total responsabilidad del control de confiabilidad, mensajes duplicados o perdidos, retardos y paquetes fuera de orden.
- Puede ser utilizado por aplicaciones que necesitan soporte de tráfico multicast o broadcast.
- No suministra ningún mecanismo de control de flujo o control de congestión.
- En caso de congestión en la red parte de los datagramas serán descartados por la red sin informar por ningún mecanismo al emisor, ni al receptor.
- En caso de saturación del receptor, éste sencillamente ignorará los datagramas que no pueda aceptar.
- Se utiliza en el entorno de la red local donde la tasa de errores de transmisión es muy pequeña.
- Se usa para programas que sólo envían mensajes cortos y pueden reenviar el mensaje si una respuesta no se produce en periodo corto de tiempo.

3.5 FORMATO UDP

Los campos *puerto origen* y *puerto destino* contienen los números de puerto del protocolo UDP. El primero de ellos es opcional. En caso de utilizarse especifica la parte a la que se tienen que enviar las respuestas, de lo contrario, puede tener valor cero.

Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.

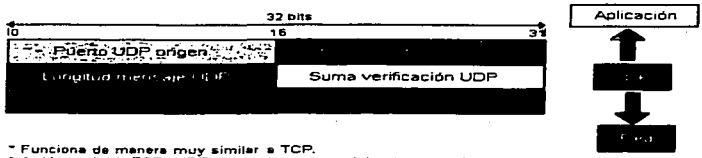
Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.

Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.

Suma de verificación UDP (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una *pseudo-cabecera* que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.

Datos. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

Formato UDP



- Funciona de manera muy similar a TCP.
- A diferencia de TCP, UDP proporciona un servicio sin conexión, pues no se realizan confirmaciones.
- Tampoco se numeran los mensajes, por lo que pueden arrivar en desorden.
- Sin embargo si manejan los sockets de la misma manera que en TCP.
- Es utilizado por aplicaciones de audio sobre la internet como Real Audio.

Fig. 3-4 Formato del Protocolo UDP (User Datagram Protocol)

FUNCIONES:

- Segmentar la información que envía la capa de aplicación, para enviarlos a la capa de red.
- Simular una comunicación orientada a conexión.
- Verificar que el segmento enviado llegue a su destino.
- Confirmar la recepción de segmentos.
- Verificar que la información llegue libre de errores a su destino.
- Ordenar los paquetes que recibe.
- Regular el flujo de información.

3.5.1 PROBLEMÁS DE UDP

Cuando una aplicación adquiere un puerto UDP, el software de red necesita reservar un buffer de suficiente tamaño de memoria para albergar toda la información que llegara a dicho puerto, ya que como UDP es un protocolo no orientado a conexión, no existe ninguna forma de indicar el número de bytes que se van a recibir.

3.6 DIFERENCIAS TCP Y UDP

Existen numerosas diferencias entre UDP y TCP. En primer lugar, TCP es protocolo orientado a conexión, lo cual requiere que ambos extremos estén de acuerdo en participar en el intercambio de datos o información. TCP es fiable, ya que numera los bytes que se envían en cada segmento evitando así la duplicidad de los datos. Además, TCP valida la información que le llega mediante el envío de segmentos cuyo bit ACK va activo permitiendo así un flujo de datos ordenado.
UDP por su parte es un protocolo simple, no orientado a conexión y que no garantiza la entrega de los datos debido a que no utiliza ninguna técnica de acuse de recibo.

Tabla 3-1 Puertos Bien Conocidos

APLICACIÓN	PUERTO	UDP	TCP
FTP	21		
TELNET	23		
SMTP	25		
DNS	53		
BOOTP	67		
WWW-HTTP	80		
POP3	110		
SFTP	115		
NTP	123		
SNMP	161		

Tabla 3-1 Utilización de TCP o UDP en algunos protocolos de aplicación y sus puertos de asignación.

Se puede observar que existen protocolos de aplicación, que pueden utilizar ambos protocolos.

Los puertos bien conocidos (well-know) son aplicaciones servidoras que utilizan unos números prefijados, en esta tabla se encuentran los más usuales.

Sin embargo existen otras diferencias que permiten el uso de uno u otro en determinadas ocasiones:

- UDP permite el envio de información mediante la técnica denominada B*roadcast*.
- UDP utiliza menos cantidad de datagramas para llevar a cabo una solicitud y una respuesta, por lo que permite que el intercambio de información, en definitiva, sea más rápido.
- TCP detecta la perdida y duplicidad de paquetes gracias a los números de secuencia.
- TCP es capaz de informar al otro extremo a cerca de la cantidad de memoria que tiene reservada para almacenar la información que espera recibir.

Una vez analizadas las principales diferencias es posible determinar las situaciones en las que es preferible la utilización de un protocolo u otro.

- UDP es necesario en las aplicaciones que requieran envios múltiples, es decir, mediante las técnicas *broadcast* y *multicast*.
- UDP es útil cuando la aplicación que sé esta manejando requiera únicamente conexiones para realizar peticiones y recibir respuestas en las que la cantidad de información que viaja por la red es pequeña.
- TCP es necesario en el envio de gran cantidad de información, donde sea necesario llevar un control de flujo, detección de segmentos duplicados y perdidos.

CAPITULO 4
INTERNET IPv6

4.1 PROTOCOLO IP v6

El protocolo IPv6 conserva muchas de las características que contribuyeron al éxito del IPv4, de hecho, los diseñadores han caracterizado al IPv6 como si fuera básicamente el mismo que el IPv4 con unas cuantas modificaciones.

El IPv6 todavía soporta la entrega sin conexión (permite que cada datagrama sea ruteado independientemente), permite al emisor seleccionar el tamaño de un datagrama y requiere que el emisor especifique el máximo número de saltos que un datagrama puede realizar antes de ser eliminado.

El IPv6 conserva la mayor parte de los conceptos proporcionados por la versión IPv4, incluyendo capacidades de fragmentación y ruteo de fuente. A pesar de las similitudes conceptuales, el IPv6 cambia la mayor parte de los detalles del protocolo.

El IPv6 utiliza direcciones largas y añade unas cuantas características nuevas. IPv6 revisa completamente el formato de los datagramas, remplazando el campo de opción de longitud variable del IPv4 por una serie de encabezados de formato fijo.

4.2 LOS CAMBIOS EN EL IPv6

Direcciones más largas. Mayor número de bits para direccionar los *host*. El IPv6 cuadruplica el tamaño de las direcciones del IPv4, va de 32 bits a 128 bits. El espacio de direcciones del IPv6 es tan grande que no podrá agotarse en un futuro previsible.

Formato de encabezados flexible. El IPv6 utiliza un formato de datagrama incompatible y completamente nuevo. A diferencia del IPv4, que utiliza un encabezado de datagrama de formato fijo en el que todos los campos excepto las opciones ocupan un número fijo de octetos en un desplazamiento fijo, el IPv6 utiliza un conjunto de encabezados opcionales.

Opciones mejoradas. Como el IPv4, el IPv6 permite que un datagrama incluya información de control opcional. El IPv6 incluye nuevas opciones que proporcionan capacidades adicionales no disponibles en el IPv4.

Soporte para asignación de recursos. El IPv6 reemplaza la especificación del tipo de servicio del IPv4 con un mecanismo que permite la preasignación de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones como video en tiempo real que requieren de una garantía de ancho de banda y retardo.

Provisión para extensión de protocolo. Posiblemente el cambio más significativo en el IPv6 es el cambio de un protocolo que especifica completamente todos los detalles a un protocolo que puede permitir características adicionales. La capacidad de extensión tiene la posibilidad de permitir que el IETF se adapte a los protocolos para cambiar al hardware de red subyacente o a nuevas aplicaciones.

4.3 DIRECCIONAMIENTO EN IP v6

El IPv6 asocia una dirección con una conexión de red especifica, no con una computadora especifica. Así, la asignación de direcciones es similar para el IPv4: un ruteador IPv6 tiene dos o más direcciones y un anfitrión IPv6, con una conexión de red, necesita sólo una dirección. El IPv6 también conserva (y extiende) la jerarquía de direcciones del IPv4 en la que una red física es asignarla a un prefijo, para hacer la asignación de direcciones y la modificación más fácil, el IPv6 permite que varios prefijos sean asignados a una red dada y que una computadora tenga varias direcciones simultaneas para asignarlas hacia una interfaz determinada.
Además de permitir varias direcciones simultaneas por conexión de red, el IPv6 expande y en algunos casos, unifica las direcciones especiales del IPv4. En general, una dirección de destino en un datagrama cae dentro de una de tres categorías:

Unicast: la dirección de destino especifica una sola computadora (anfitrión o ruteador); el datagrama deberá rutearse hacia el destino a lo largo de la trayectoria más corta.

Multicast: especifica un grupo de interfases de red. Este mecanismo se utiliza frecuentemente en la videoconferencia, ya que cada grupo de interfaces incluye múltiples interfaces de diferentes sistemas y cuando un mensaje (o imagen) es enviado a través de Multicast, la propia red es la encargada de que el mensaje llegue a su destino.

Anycast: es nuevo en el IPv6. Una dirección Unycast identifica a una entre un conjunto de interfaces (puede contener interfaces de diferentes sistemas). Por lo tanto el funcionamiento es parecido al Multicast, con la diferencia que el Anycast se refiere a una interfaz del conjunto global y no a todas las interfaces del grupo.

4.4 FORMATO DE DIRECCIONES IP v6

El formato de direcciones tiene la siguiente estructura:

XXXX:YYYY:ZZZZ:XXXX:YYYY:ZZZZ:XXXX:YYYY

La notación de las direcciones IPv6 es la siguiente:

Se trata de ocho grupos de 16 bits, cuatro dígitos hexadecimales, separados por dos puntos.

Por ejemplo:

8000:0000:0000:0000:0123:4567:89AB:CDEF.

Para abreviar la gran cantidad de ceros que tenga una dirección se puede utilizar una notación abreviada, en la que los ceros a la izquierda pueden omitirse, y además, si uno o más grupos tienen todos los dígitos en cero se pueden omitir poniendo en su lugar dobles dos puntos.

Volviendo al caso anterior:

8000::123:4567:89AB:CDEF

Para evitar ambigüedades, la notación abreviada :: sólo puede utilizarse una vez en una dirección. Ya que el campo dirección en IPv6 es más largo, se puede reservar los seis últimos bytes de la dirección para incluir una parte local globalmente única en la dirección, que típicamente es una dirección MAC IEEE (esto es similar al direccionamiento usado en ATM), lo que permite la auto configuración de los nodos, pues éste fija la parte local de su dirección y a partir de la dirección contenida en su tarjeta de red, escucha por el cable para que el router le informe de la parte de red, configurando automáticamente al nodo y garantizando que la dirección es única.

Una dirección Internet de IPv4 como, por ejemplo, 192.168.100.1, podría representarse en IPv6 como:

:: 192.168.100.1

4.5 FORMATO DE CABECERA IP v6

Un encabezado base IPv6 contiene menos información que un encabezado de datagrama IPv4. Las opciones y algunos de los campos fijos que aparecen en un encabezado de datagrama del IPv4 se han cambiado por encabezados de extensión en el IPv6. En general, el cambio en los encabezados en los datagramas refleja los cambios en el protocolo:

- La alineación se ha cambiado de múltiplos de 32 bits a múltiplos de 64 bits.
- Los campos de longitud de encabezado se han eliminado y el campo de longitud de datagrama ha sido reemplazado por el campo *PAYLOAD LENGTH (LONGITUD PAYLOAD).*
- El tamaño de los campos de dirección de fuente y destino se ha incrementado en 16 octetos cada uno.
- La información de fragmentación se ha movido de los campos fijos en el encabezado base, hacia un encabezado de extensión.
- El campo *TIME-TO-LIVE (LIMITE DE SALTO)* ha sido reemplazado por el *HOP LIMIT.*
- El campo *SERVICE TYPE* ha sido reemplazado por el campo *FLOW LABEL (ETIQUETA DE FLUJO).*
- El campo *PROTOCOL* ha sido reemplazado por un campo que especifica el tipo del próximo encabezado *(NEXT HEADER).*

FORMATO DE CABECERA DE IPv6

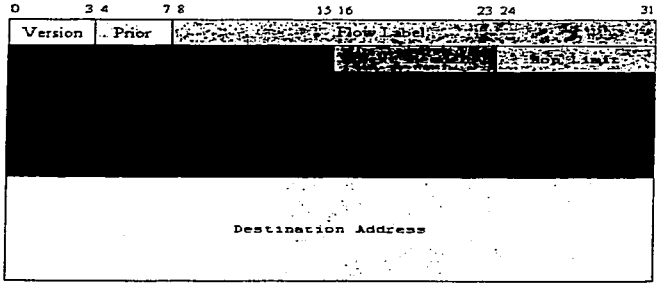


Fig. 4-1 Formato de cabecera del IPv6

Versión.

Este campo de 4 bits indica la versión del Protocolo IP. En este caso tendrá un valor de 6.

Se encuentra en la misma posición que en los datagramas IPv4, por lo que un sistema que se encuentre preparado para trabajar con IPv4 e IPv6 podrá diferenciar los datagramas de ambas versiones.

Prioridad.

La utilidad y valores que puede tomar este campo es aún materia de investigación. Inicialmente se añadió la cabecera para poder identificar la prioridad de los datagramas, diferenciando él trafico que puede ser descartado en caso de congestión, en él trafico urgente y sensible a los retrasos, etc.

Etiqueta de Flujo.

Contendrá un valor aleatorio elegido por la aplicación. El IPv6 define el concepto de flujo como una secuencia de paquetes enviados desde un sistema de origen a uno destino, donde el sistema de origen especifica que los paquetes deben ser tratados de forma especial por aquellos *routers* que los encaminen. En el uso de este campo experimental.

Tamaño de la Carga.

Tamaño en bytes de toda la información que va a continuación de la cabecera IPv6. Un valor 0 en este campo especifica que no se tiene suficiente con 16 bits para representar el tamaño, sino que este se indicará en una cabecera adicional que se envía después de la cabecera IPv6 estándar.

2 Bytes que indican el tamaño del paquete en bytes, sin considerar los 40 Bytes de encabezado. Como el valor máximo codificable es 65535, el paquete máximo será de 65575.

Siguiente Encabezado.
1 Byte que sirve para indicar si el encabezado está seguido por alguno de los encabezados opcionales. Si no existen opciones, este campo indica el protocolo de nivel de transporte al que pertenece el paquete, utilizando los mismos códigos que en IPv4.

Límite Saltos.
1 Byte equivalente al campo TTL de IPv4, donde el máximo número de saltos especificables es 255. Cada router que encamina el datagrama decrementará en uno esté campo, descartando el paquete si llega a 0

Dirección Fuente y Dirección Destino.
16 Bytes para especificar la IPv6 del nodo fuente y 16 Bytes para especificar la IPv6 del nodo destino, con la diferencia de que ahora son campos de 128 bits.

4.6 CABECERAS DE EXTENSIÓN

Cada paquete IPv6 incluye encabezados de extensión sólo para los requerimientos necesarios del paquete. Cada encabezado de base y opcional contiene un campo siguiente encabezado para indicar el tipo del siguiente encabezado. Para extraer toda la información del encabezado de un paquete IPv6 se requiere procesar secuencialmente todos los encabezados. Los routers intermedios no necesariamente necesitan procesarlos todos. Algunos tipos de encabezados IPv6 posibles son los siguientes:

Salto-a-Salto.
Entrega información que debe ser examinada por todos los routers por los que pase el paquete. Hasta el momento se ha definido sólo una opción a este encabezado y permite especificar paquetes de longitud superior a 64 Kbytes, que pueden llegar a tener hasta 4 Gbytes.

Routing.
Realiza las funciones combinadas de Strict y Loose Source Routing de IPv4. El máximo número de direcciones que puede especificarse es de 24.

Fragment.
Utilizada cuando se deba fragmentar un paquete. El mecanismo utilizado es similar al de IPv4, con la diferencia de que en IPv6 sólo se permite la fragmentación en el origen. De esta forma, se simplifica notablemente la complejidad de proceso en los routers.

Authentication.
Permite el uso de encriptación para incorporar un mecanismo de firma digital por el cual el receptor del paquete puede estar seguro de la autenticidad del emisor.

Encrypted Security Payload.
Permite el envío de información encriptada que sólo pueda ser leída por el destinatario. La encriptación afecta sólo a los datos, ya que ésta ha de ser leída e interpretada por cada router por el que pasa.

CONCLUSIONES

El protocolo TCP/IP es el más viejo, por la amplia estructura que ofrece, ha contribuido a la exitosa operación de una red a nivel mundial.

La estructura principal del protocolo TCP /IP se basa en el modelo de referencia OSI (Interconexión de Sistema Abierto), OSI ofrece varios productos sofisticados que TCP / IP ha utilizado para mejorar las operaciones en la estructura de los principales protocolos de comunicación.

Un protocolo de comunicación esta optimizado para enlazar cualquier tipo de red (WAN, LAN, MAN, Anillo, X.25, Ethernet, etc.). Cuando varias redes son enlazadas, el punto de infraestructura dentro de este sencillo sistema es la estructura principal de la red. El modelo de referencia OSI y el protocolo TCP /IP únicamente contienen algunas propiedades de la estructura de los principales protocolos de comunicación.

Un ejemplo muy notable es de que tan útil es TCP / IP es la gran cantidad de computadoras que están conectadas a cualquier red para compartir información a través de Internet.

Internet ha crecido dentro de la Red Internacional de Redes que utilizan TCP/IP para enlazar diferentes dispositivos de comunicación y sin comparar los sistemas de las computadoras.

Las redes son unidas dentro de Internet por Routers (algunas veces llamados gateways) que típicamente trabajan en el protocolo IP en función de TCP / IP.

La serie de protocolos que representan el protocolo TCP / IP son tres capas de servicios de comunicación, estos servicios conceptualmente descansan en una cuarta capa (Capa de Aplicación), la cual pertenece al hardware usado para la transmisión de datos.

En la **Capa de Aplicación** se encuentran una serie de protocolos que realizan distintas tareas de red, las cuales son muy utilizadas en Internet. Estas aplicaciones se ven controladas por los siguientes protocolos:

FTP: File Transfer Protocol (Protocolo de Transporte de Archivos).

TELNET: Protocolo de Servicio de Conexión Remota (Remote Login).

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

SMTP: Simple Mail Transport Protocol (Protocolo de Transporte de Correo Simple).

DNS: Domain Name Service (Servicio de Nombre de Dominio).

TFTP: Trival File Transport Protocol (Protocolo de Transporte de Archivo Trivial).

WWW: World Wide Web.

En la **Capa de Transporte** aparecen dos protocolos importantes:

El protocolo **TCP** proporciona un servicio de comunicación que forma un circuito virtual, el cual es llamado una conexión. TCP tiene un servicio de conexión entre los programas llamados y los que llaman, un chequeo de errores, control de flujo y capacidad de interrupción.

El protocolo **UDP** es más simple que **TCP** porque no se preocupa por los mensajes que se pierden, el orden en que se envían, etc. UDP se utiliza sólo para programas que envían mensajes cortos (Multicast y Broadcast) y puede reenviar mensajes si una respuesta no se produce en un periodo corto de tiempo. El UDP también se utiliza en torno de red local donde los errores de transmisión son muy pequeños y no es necesario el sofisticado control de errores del protocolo TCP.

En la **Capa de Red o Internet**, el protocolo principal es IP, pero existe otro protocolo el ICMP.

IP ofrece las herramientas necesarias para el envío de datagramas, pero no ofrece los medios para garantizar la integridad de dichos datagramas y que estos alcancen su destino. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP / IP es el datagrama.

Los datagramas pueden ser retrasados, duplicados, perdidos, enviados en una secuencia incorrecta y es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje y algunas ocasiones estos son recibidos en las máquinas de origen.

El protocolo IP también define cual será la ruta inicial por la cual serán mandados los datos.

ICMP(Protocolo Control de Mensaje Internet) no puede hacer que IP sea más fiable, pero ofrece la posibilidad de que un gateway, un router o un host destino comuniquen al de origen cuando ha existido algún problema con el datagrama que se ha enviado.

Los mensajes ICMP viajan por la red dentro del campo de datos de IP. En la cabecera IP el campo de protocolo establece a 1 para indicar que viaja dentro del mensaje ICMP.

En la **Capa Física** corresponde el hardware donde están los protocolos **ARP** y **RARP**.

El protocolo **ARP** (Address Resolution Protocol), es el encargado de convertir las direcciones IP en direcciones de la red física. El funcionamiento del protocolo ARP es muy simple, cuando una máquina origen desea enviar un mensaje a otra máquina que

esta conectada en una red diferente se encuentra con el problema de la dirección de la máquina es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP por medio de una Tabla de Direcciones ARP, que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas.

El protocolo **RARP** (Reverse Address Resolution Protocol) es el encargado de asignar una dirección IP a una dirección física.

La próxima generación de IPv6 tiene cambios importantes donde los protocolos IP e ICMP son completamente modificados, la interfaz de programación cambia un poco. Se caracteriza porque maneja direcciones de 128 bits, tiene un soporte para tiempo real y multimedia (Audio y Video), una mayor seguridad y un ruteo más eficiente.

ANEXO A:

GLOSARIO DE TÉRMINOS Y ABREVIATURAS

ACKNOWLEDGEMENT(ACK Reconocimiento o Acuse de Recibo)
Respuesta enviada por un receptor para indicar que recibió con éxito la información que le fue enviada. Los acuses de recibo se pueden implantar en cualquier nivel, incluyendo el nivel físico (utilizando el voltaje en uno o más cables para coordinar la transferencia), en el nivel de enlace (para indicar la transmisión exitosa a través de un sólo enlace de hardware) o en niveles elevados (por ejemplo, para permitir que un programa de aplicación, en el destino final, responda a un programa de aplicación en la fuente).

ADDRESS MÁSK (Máscara de Dirección)
Máscara de bits utilizada para seleccionar bits de una dirección IP a fin de direccionar subredes. La máscara es de 32 bits de longitud y selecciona la porción de red de la dirección IP así como uno o más bits de la parte local.

ADDRESS RESOLUTION (Resolución de Dirección)
Conversión de una dirección de protocolo en su correspondiente dirección física (por ejemplo, la conversión de una dirección IP en una dirección Ethernet). Dependiendo de la red subyacente, la resolución puede requerir difusión en una red local.

ANS (Advanced Networks and Services)
Compañía propietaria y operadora de la columna vertebral de la red de Internet en 1995.

ANSI
(American National Standards Institute) Grupo que define los estándares de Estados Unidos para la industria del procesamiento de información. ANSI participa en la definición de los estándares de protocolos de red.

ANSNET
Red de área amplia que formaba la red de columna vertebral de Internet en 1995.

ARP *(Address Resolution Protocol)*
Protocolo TCP/IP utilizado para asignar una dirección IP de alto nivel a una dirección de hardware físico de bajo nivel. ARP se utiliza a través de una sola red física y esta limitada a redes que soportan difusión de hardware.

ARPA *(Advanced Research Projects Agency)*
Institución gubernamental que fundo la ARPANET y después, la red global Internet. El grupo dentro de ARPA responsable de ARPANET. ARPA se conoció como *DARPA* por varios años.

ARPANET
Red pionera de gran alcance fundada por ARPA (después DARPA). Sirvió de 1969 a 1990 como base para las primeras investigaciones de red y como columna vertebral de red durante el desarrollo de Internet. ARPANET consiste en nodos individuales conmutadores de paquetes interconectados por líneas arrendadas.

ATM *(Asynchronous Transfer Mode)*
Tecnología de red orientada a la conexión que utiliza pequeñas celdas de tamaño fijo en la capa de nivel inferior. ATM tiene la ventaja potencial de ser capaz de soportar voz, video y datos con una sola tecnología subyacente.

AUTHENTICATION HEADER(AH)
Cabecera de Autentificación para **IPv6.**

BACKBONE NETWORK (Red de Columna Vertebral de la Red)
Cualquier red que forme la interconexión central para una red de redes. Una columna vertebral de red nacional es una WAN; una columna vertebral de red corporativa puede ser una LAN.

BASE HEADER (Encabezado Base)
En la propuesta **IPng**, es el encabezado que se encuentra al comienzo de cada datagrama.

BRIDGES (Puentes)
Dispositivos que además de copiar bits desde un extremo al otro, analizan las cabeceras del nivel de enlace.

CHECKSUM (Suma de Verificación)
Número entero calculado a partir de una secuencia de octetos que son tratados como enteros en una suma para calcular su valor total. Una suma de verificación se utiliza para detectar errores que aparecen cuando una secuencia de octetos se transmite de una máquina a otra. Por lo general, el software de protocolo calcula una suma de verificación y la anexa al paquete que sé esta transmitiendo. En la recepción, el software de protocolo verifica el contenido del paquete recalculando la suma de verificación y comparándolo con el dato obtenido de la transmisión.
Muchos protocolos TCP/IP utilizan una suma de verificación de 16 bits, calculada por complemento aritmético a uno, con todos los campos enteros en el paquete almacenados en el orden de octetos de la red.

CLIENT-SERVER (Cliente-Servidor)
Modelo de interacción en un sistema distribuido en el que un programa, en una localidad, envía una solicitud a otro programa en otra localidad y espera una respuesta. El programa solicitante se conoce como cliente, el programa que atiende la solicitud como servidor. Es común que se estructure primero el software cliente y después el servidor.

CONNECTION (Conexión)
Abstracción proporcionada por el software de protocolo. El TCP ofrece una conexión de una aplicación en una computadora a la aplicación en otra.

DARPA
(Defense Advanced Research Projects Agency) Nombre anterior de ARPA.

DATAGRAM (Datagrama)
Son bloques de datos en los que se divide la información.

DEMULTIPLEX (Demultiplexor).
Dispositivo que separa una entrada común en varias salidas. El demultiplexado se presenta en muchos niveles. El hardware demultiplexa señales de una línea de transmisión basada tiempo o en una frecuencia portadora para permitir varias transmisiones simultaneas a través de un sólo cable físico. El software demultiplexa los datagramas entrantes enviando cada 1 hacia él modulo de protocolo de alto nivel apropiado o a un programa de aplicación.

DHCP *(Dynamic Host Configuration Protocol)*
Protocolo utilizado por un anfitrión para obtener toda la información de configuración necesaria incluida en una dirección IP.

DNS *(Domain Name System)*
Sistema de base de datos distribuida en línea y utilizado para transformar nombres de máquina en direcciones IP que puedan leer los usuarios. Los servidores DNS, a través de Internet, implantan un espacio de nombres jerárquico que permite a las calidades contar con libertad para asignar nombres de máquinas y direcciones. DNS también soporta transformaciones separadas entre destinos de correo y direcciones IP.

DOMAIN (Dominio)
Parte de una jerarquía de nombres. Sin tácticamente, un nombre de dominio consiste en secuencia de nombres (etiquetas) separadas por puntos.

ENCAPSULATING SECURITY PAYLOAD HEADER
Cabecera de Seguridad para **IPv6.**

ENCAPSULATION (Encapsulación)
Técnica utilizada por los protocolos estratificados por capas en la cual un protocolo de nivel inferior acepta un mensaje de un protocolo de nivel superior y lo coloca en la sección de datos de su trama de bajo nivel. La encapsulación implica que los datagramas que viajan a través de una red física cuentan con una secuencia de encabezados de los que el primero proviene de la trama de red física, el siguiente del Protocolo Internet (IP), el siguiente del Protocolo de Transporte y así sucesivamente.

ETHERNET
Popular tecnología de red de área local, Ethernet es un cable coaxial pasivo; las interconexiones contienen todos los componentes activos. Ethernet es un sistema de entrega.
El estándar para Ethernet es 10 Mbps. Originalmente, Ethernet utilizaba un cable coaxial. En versiones posteriores empezó a utilizar un cable coaxial delgado *(Thinnet)* o un cable de par trenzado (Base-T).

FLOW CONTROL (Control de Flujo)
Control de la razón de transferencia a la que introducen los anfitriones y los ruteadores paquetes en una red a en una red de redes, por lo general para evitar congestionamientos.

GATEWAYS (Pasarelas)
Utilizadas para conectar redes WAN. Trabajan a nivel de aplicación.

HOP BY HOP
Opciones salto a salto para **IPv6.**

HOSTID (Identificador de Host)

ICMP *(Internet Control Message Protocol)* ***Protocolo De Mensajes De Control y Error***
Parte integral del protocolo de Internet (IP) que resuelve errores y controla los mensajes. Específicamente, los anfitriones y los ruteadores utilizan el ICMP para enviar reportes de problemas relacionados con datagramas que se devuelven a la fuente original que envia el datagrama. El ICMP también incluye una solicitud / replica de eco utilizada para probar si un destino es accesible y responde.

IGMP (*Internet Group Management Protocol)*
Protocolo que utilizan los anfitriones para mantener a los ruteadores locales informados de sus miembros y de sus grupos de multidifusión. Cuando todos los anfitriones abandonan un grupo, los ruteadores no envian los datagramas que lleguen para el grupo.

ISO International Organization for Standardization

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)
Organización Internacional que establece los estándares para la interconexión del equipo telefónico. Esta definió el estándar para el protocolo de red X.25

INTERNET (Red de redes)
Físicamente, una conexión de redes de conmutación de paquetes interconectadas por ruteadores, junto con los protocolos TCP/IP permiten que la red funcione como una sola red virtual extensa. Cuando se escribe con mayúscula, Internet se refiere específicamente a la red global de Internet.

INTERNET
Conjunto de redes y ruteadores que abarca 61 países y utiliza los protocolos TCP/IP para formar una sola red virtual cooperativa. Internet conecta más de cuatro millones de computadoras.

INTERNET ADDRESS (Dirección Internet)

INTERNET PROTOCOL (Protocolo de Internet)

IP (Internet Protocol)
Protocolo estándar que define a los datagramas IP como la unidad de información que pasa a través de una red de redes y proporciona las bases para el servicio de entrega de paquetes sin conexión y con el mejor esfuerzo. El IP incluye el control ICMP y los protocolos de mensaje de error como parte integral. El conjunto de protocolos completo se conoce frecuentemente como TCP/IP y son los dos protocolos más importantes.

IP ADDRESS (Dirección IP)
Dirección de 32 bits asignada a cada anfitrión que participa en una red de redes TCP/IP. Una dirección IP es una abstracción de la dirección de hardware físico. Para hacer el ruteo eficiente, cada dirección IP se divide parte en red y parte en anfitrión.

IP DATAGRAM (Datagrama IP)
Unidad básica de información que pasa a través de una red de redes TCP/IP. Un datagrama IP es a una red de redes lo que un paquete de hardware es a una red física. Contiene las direcciones de fuente y destino junto así como los datos.

IPng (Internet Protocol -the Next Generation)
Termino aplicado a todas las actividades alrededor de la especificación y la estandarización de la próxima versión del IP.

IPv4
Sinónimo de la versión actual del IP.

IPv6
Nombre oficial de la próxima versión del IP.

ISO (International Organization for Standardization)
Organización internacional que discute, propone y especifica estándares para los protocolos de red. ISO es mejor conocido por su modelo de referencia de siete capas que describe la organización conceptual de los protocolos. Aun cuando se propuso como un conjunto de protocolos para la interconexión de sistemas abiertos, los protocolos OSI no han sido ampliamente aceptados a nivel comercial.

ITU- Ts
Abreviatura de *Telecommunication Section* de la *International Telecommunication Union.*

JUMBO PAYLOAD
Opciones de destino para IPv6.

Kbps (Kilo Bits Per Second)
Medida de la cantidad de datos transmitidos.

LAN *(Local Area Network)*
Cualquier tecnología de red física diseñada para cubrir distancias cortas (del orden de unos cuantos cientos de metros). Por lo general las LAN operan a velocidades que van de los diez millones de bits por segundo a varios gigabits por segundo. Algunos ejemplos incluyen las redes Ethernet.

Mbps *(Millions of Bits Per Second o millones de bits por segundo)*
Medida de la cantidad de datos transmitidos.

MILNET *(MILitary NETwork, Red Militar)*
Originalmente parte de ARP ANET , MILNET se separó en 1984.

MIME *(Multipurpose Internet Mail Extensions)*
Estándar utilizado para codificar datos como imágenes, en texto ASCII, para su transmisión a través del correo electrónico.

MTU (Maximum Transfer Unit)
La mayor cantidad de datos que se puede transferir por unidad a través de una red física dada. El MTU lo determina el hardware de red.

MULTICAST (Multidifusión)
Técnica que permite que copias de un sólo paquete se transfieran a un subconjunto seleccionado de todos los posibles destinos. Algunos tipos de hardware (por ejemplo, Ethernet) soportan la multidifusión y permiten que una interfaz de red pertenezca a uno o más grupos de multidifusión. El IP soporta una capacidad de multidifusion de red de redes.

NETID (Identificador de Red)

NSF *(National Science Foundation)*
Dependencia gubernamental de Estados Unidos que inició algunas de las investigaciones y desarrollos de Internet.

NSFNET *(National Science Foundation NETwork)*
Se utiliza para describir la red de columna vertebral en Estados Unidos, que es administrada por la NSF.

OSI *(Open Systems Interconnection) INTERCONEXION DE SISTEMÁS ABIERTOS*
Se trata de los protocolos, específicamente estándares de ISO, para la interconexión de sistemas de computadoras cooperativos.

PACKET (Paquete)
Se trata, en términos generales, de cualquier bloque pequeño de datos enviado a través de una red de conmutación de paquetes.

PADDING (Relleno)
Este campo consiste en un número de octetos (de uno a tres), que tienen valor cero y sirven para que la longitud de la cabecera sea divisible por cuatro.

PING *(Packet InterNet Groper)*
Nombre de un programa utilizado con las redes de redes TCP/IP que se usa para probar la accesibilidad de un destino, enviando una solicitud de eco ICMP y esperando una respuesta.

PROTOCOL PORT (Protocolo de Puerto)
Abstracción que los protocolos de transporte del TCP/IP utilizan para distinguir entre varios destinos sin una computadora anfitrión dada. Los protocolos TCP/IP identifican puertos mediante el uso de enteros positivos pequeños. Usualmente el sistema operativo permite a un programa de aplicación especificar que puerto desea utilizar. Algunos puertos se reservan para servicios estándar (ejemplo, el correo electrónico).

PSEUDO HEADER (Pseudo Encabezado)
Información de direcciones IP de fuente y destino enviadas en el encabezado IP, pero incluidas en un TCP o en suma de verificación UDP.

PUSH (Empujar)
Operación que realiza una aplicación en una conexión TCP para forzar a que un dato se envié inmediatamente. Un bit en el encabezado de segmento marca el dato que se esta empujando.

RARP *(Reverse Address Resolution Protocol)*
Protocolo TCP/IP que una máquina sin disco utiliza al arrancar para encontrar su dirección IP. La máquina difunde una solicitud que contiene su dirección de hardware físico y un servidor responde enviando a la máquina su dirección IP. RARP toma su formato de nombre y mensaje de otro protocolo de resolución de dirección IP, ARP.

REASSEMBLY (Reensamblado)
Proceso de reunir todos los fragmentos de un datagrama IP y utilizarlos para crear una copia del datagrama original. El destino final realiza el reensamblado.

REDIRECT (Redireccionamiento)
Mensaje ICMP enviado de un ruteador a un anfitrión en una red local para instruir al anfitrión a que cambie de ruta.

RLOGIN (Remote LOGIN)
Protocolo de acceso remoto desarrollado para UNIX por Berkeley. Rlogin ofrece esencialmente el mismo servicio que TELNET.

ROUTE (Ruta)
En general, una ruta es la trayectoria que él trafico de red toma de su fuente a su destino. En una red de redes TCP/IP, cada datagrama IP es ruteado de manera independiente; las rutas pueden cambiar dinámicamente.

ROUTER (Ruteador)
Computadora dedicada, de propósito especial, que se conecta a dos o más redes y envía paquetes de una red a otra. En particular, un ruteador IP envía datagramas IP entre las redes a las que esta conectado. Un ruteador utiliza las direcciones de destino en un datagrama para decidir el próximo salto al que enviará el datagrama.

SEGMENT(Segmento)
Unidad de transferencia enviada del TCP en una máquina al TCP en otra. Cada segmento contiene parte de un flujo de octetos, que son enviados entre las máquinas, así como campos adicionales que identifican la posición actual en el flujo y una suma de verificación que asegura la validez de los datos recibidos.

SMTP *(Simple Mail Transfer Protocol)*
Protocolo estándar del TCP/IP para transferir mensajes de correo electrónico de una máquina a otra. SMTP especifica como interactúan dos sistemas de correo y el formato de los mensajes de control que intercambian para transferir el correo.

SNMP *(Simple Network Monitoring Protocol)*
Protocolo estándar utilizado para monitorear anfitriones, ruteadores y las redes a las que están conectados.

SOCKET
Abstracción proporcionada por el sistema operativo UNIX que permite a un programa de aplicación accesar los protocolos TCP/IP.

SOURCE ROUTE (Ruta de Fuente)
Ruta que se determina por la fuente. En el IP, una ruta de fuente consiste en una lista de ruteadores que un datagrama debe visitar; el ruteador se especifica como una opción IP. La ruta de fuente se utiliza casi siempre para depuración.

SYN*(Synchronizing segment)*
Primer segmento enviado por el protocolo TCP, se utiliza para sincronizar los dos extremos de una conexión en la preparación de una conexión abierta.

TCP *(Transmission Control Protocol)* ***Protocolo de Control de Transmisión***
Protocolo de nivel de transporte TCP/IP estándar que proporciona el servicio de flujo confiable full duplex y del cual dependen muchas aplicaciones. El TCP/IP permite que el proceso en una máquina envié un flujo de datos hacia el proceso de otra. El TCP está orientado a la conexión en el sentido de que, antes de transmitir datos, los participantes deben establecer la conexión. Todos los datos viajan en segmentos TCP, en donde cada viaje se realiza a través de Internet en un datagrama IP. El conjunto de protocolos

completo se conoce frecuentemente como TCP/IP debido a que el TCP y el IP son los dos protocolos más importantes.

TCP/IP (Internet Protocol Suite)
Nombre oficial de los protocolos TCP/IP.

TELNET
Protocolo estándar del TCP/IP para servicio de terminal remota. TELNET permite al usuario en una localidad interactuar con un sistema de tiempo compartido remoto como si el teclado y el monitor del usuario estuvieran conectados a la máquina remota.

TFTP (Trivial File Transfer Protocol)
Protocolo estándar TCP/IP para transferencia de archivos con capacidad mínima y sobrecarga mínima. El TFTP depende sólo del servicio de entrega de datagramas sin conexión y no confiable (UDP) de este modo, puede utilizarse en máquinas como las estaciones de trabajo que conservan el software en ROM y lo utilizan para arrancar.

TOKEN RING
Cuando se utiliza en sentido genérico, se refiere a un tipo de tecnología de red que controla el acceso de medios pasando un paquete distintivo, llamado token (ficha) de máquina en máquina. Una máquina puede transmitir un paquete sólo cuando tiene la ficha (Token). Cuando se utiliza con un sentido específico, se refiere al hardware de red token ring producido por IBM.

TOS *(Type Of Service)*
Cada encabezado de datagrama IP incluye un campo que permite al emisor especificar el tipo de servicio deseado. En la práctica, pocos ruteadores utilizan TOS cuando eligen una ruta.

TTL *(Time To Live)*
Técnica utilizada en los sistemas de entrega con el mejor esfuerzo para evitar que los paquetes permanezcan en un ciclo por tiempo indefinido. Por ejemplo, a cada datagrama IP se le asignan tiempo límite entero cuando se crea. Cada ruteador decrementa el campo de tiempo límite cuando el datagrama llega y un ruteador descarta cualquier datagrama si el contador de tiempo límite llega a cero.

TYPE OF SERVICE ROUTING (Tipo de Ruteo de Servicio)
Esquema de ruteo en el que la elección de una trayectoria depende de las características de la tecnología de red subyacente, así como de la trayectoria más corta hacia el destino. En principio, el Protocolo Internet (IP) se adapta al tipo de servicio de ruteo debido a que los datagramas contienen un campo de solicitud de tipo de servicio. En la práctica pocos ruteadores cumplen con el tipo de servicio solicitado.

UDP (***User Datagram Protocol)***
Protocolo estándar TCP/IP que permite a un programa de aplicación en una máquina enviar un datagrama hacia el programa de aplicación en otra máquina. El UDP utiliza el Protocolo de Internet (IP) para entregar datagramas. Conceptualmente la diferencia importante entre los datagramas UDP y los IP es que el UDP incluye un número de puerto de protocolo, lo que permite al emisor distinguir entre varios programas de aplicación en una máquina remota dada. En la practica el UDP también incluye una suma de verificación opcional en el datagrama que se esta enviando.

UNICAST (Unidifusión)
Método mediante el cual un paquete se envía a un sólo destino. La mayor parte de los datagramas IP se manda vía unidifusión.

URGENT DATA (Datos Urgentes)
Método utilizado en el TCP para enviar datos fuera de banda. Un receptor procesa los datos urgentes en cuanto los recibe.

URL (*Uniform Resource Locator)*
Cadena que proporciona la localización de una parte de la información. La cadena comienza con el tipo de protocolo (por ejemplo, el FTP) seguido por la identificación de información especifica (por ejemplo, el nombre de dominio de un servidor y el nombre de la trayectoria hacia un archivo en el servidor).

VIRTUAL CIRCUIT (Circuito Virtual)
Abstracción básica proporcionada por un protocolo orientado a la conexión como el TCP. Una vez que un circuito virtual se ha creado, se establece un efecto hasta que se desactiva explícitamente.

WAN *(Wide Area Network)*
Cualquier tecnología de red que abarca distancias geográficas extensas. También llamadas redes de gran alcance, las WAN actualmente operan a bajas velocidades y tienen retardos significativamente mayores que las redes que operan sobre distancias cortas.

WELL-KNOWN PORT (Puerto Bien Conocido)
Por los protocolos nivel de transporte (es decir, TCP y UDP). Cada servidor esta en la lista de un puerto bien conocido, de este modo, sus clientes pueden localizarlo.

WINDOW (Ventana)
Este campo contiene un entero de 32 bits. Se utiliza para indicar el tamaño de buffer disponible que tiene el emisor para recibir datos.

WORKING GROUP (Grupo de Trabajo)
El término se aplica a un comité de IETF. Cada grupo de trabajo es responsable de un protocolo particular o del diseño de algún aspecto.

WWW (World Wide Web)
Servicio de información a gran escala que permite a un usuario buscar información. WWW ofrece un sistema de hipermedios que puede almacenar información como texto, gráficos, audio, etcétera.

X.25
Protocolo estándar de ITU- TS para el servicio de red a nivel de transporte. Es posible formar túneles a través de X.25.

BIBLIOGRAFÍA

Floyd Wylder.
AGuide to TCP/IP Protocol Suite.
ED. Artech House. 1993.

Jose Luis Raya, Victor Rodrigo
Domine TCP/IP.
ED. Alfaomega RA-MA 1997.

Comer E., Douglas
Redes globales de información con Internet y TCP/IP,
Tercera edición.
Prentice Hall, 1996. [Protocolos TCP/IP]

Stallings, William
Comunicaciones y redes de computadores,
Quinta edición.
Prentice Hall, 1997. [Principios de redes y comunicaciones]

Ángel López-Alejandro Novo
Protocolos de INTERNET
ED. Alfaomega RA-MA 2000. [Diseño e implementación en sistemas UNIX]

Matthew G. Naugle
Network Protocol Hand Book
Mc Graw Hill, 1994.

Walter Goralski
TCP/IP APPLICATIONS AND PROTOCOLS
Computer Technology Research Corp.
First edition, 1995.

Uyless Black
TCP/IP & RELATED PROTOCOLS
Mc Graw Hill, Second Edition, 1995.

Tenenbaum, Andrew S.
REDES DE COMPUTADORAS
Pearson , Tercera edición, 1997.