30

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
C U A U T I T L A N

"COMUNICACIONES. PROTOCOLOS TCP/IP"

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

EDGAR RAYMUNDO FRAGOSO COSSIO

ASESOR: ING. VICENTE MAGAÑA GONZALEZ

CUAUTITLAN IZCALLI, EDO. DE MEXICO 2000

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

UNIDAD DE LA ADMINISTRACION ESCOLAR

DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

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 García 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.

Comunicaciones. Protocolos TCP/IP.

que presenta el pasante: Edgar Raymundo Fragoso Cossío

con número de cuenta: 8907729-2 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 7 de septiembre de 2000

MODULO	PROFESOR	FIRMA
I	Ing. Jorge Ramírez Rodríguez	
II	Ing. Vicente Magaña González	Vicente Magaña
IV	Ing. Alfonso Contreras Márquez	Contreras Márquez Alfonso

AGRADECIMIENTOS

AGRADECIMIENTOS

Con mucho amor y respeto

A Raymundo Fragoso Gómez
In memoriam

A mi Mamá
Ma. De Jesús Cossío Acosta
que siempre esta conmigo apoyándome en todo

AGRADECIMIENTOS

A Dios, por que siempre estar a mi lado y cuidándome a cada paso.

A mi abuela María Luisa (in memoriam), por su manera muy particular de impulsarme a ser mejor.

A mi tío Juan José "Coco", por apoyarme,siempre.

A mis hermanos, Paty y Fernando, por estar siempre conmigo.

A mi primo Willy y toda la familia Camacho Santos.

A mi tía Natalia, Irma y Janda; a mis primas y primos, Sonia, Adalinda, Gaby, Macarena, Judy, Jaime, y todos los demás de la familia Cossío.

A mi tía Lupe, Doña Lupe, Don Modesto (in memoriam), Juany y Mirna.

A mis amigos de la universidad "los perros" : José Alberto, Carlos, Salvador, Guillermo, Miguel Angel, Oscar, Saul, Abel, Alfonso y a todos los demás, por ser como son, y mis amigas Magali y Lulu, por darme su cariño.

A mis buenos profesores (Juan González, Blanca de la Peña, Buendía, Cobos, etc.), por encaminarme a la superación profesional.

A mi novia Elena, por todo su amor y comprensión.

A la universidad, por brindarme la oportunidad que estudiar y ser I.M.E.

A mi asesor el Ing. Vicente Magaña, hacer posible este trabajo.

Y a todos los demás que pudieran faltar: Gracias.

INDICE

INDICE

INDICE

PROLOGO

PROLOGO

Hoy en día es muy importante la comunicación de enlace de redes. Un ejemplo es la red telefónica que esta enlazada a todo el mundo. Pero para que todos los usuarios puedan comunicarse entre si, es necesario un estándar internacional, por tal motivo desde la década de los 70´s se crearon los protocolos TCP/IP. En un principio fueron solamente de uso militar, pero como era de esperarse, tiempo después de difundieron a todo el mundo.

De este conjunto de protocolos se da el mejor entendimiento para la red internacional: INTERNET.

Como todos los sistemas de comunicaciones, los protocolos TCP/IP se actualizan, dando como resultado nuevas versiones y mejoras, sin perder su compatibilidad y eficiencia.

En este libro se verán sus inicios, que son, y como funcionan los protocolos TCP/IP, también se entenderá la comparación con el modelo OSI, el direccionamiento IP y la nueva versión de IP (IPng).

Se comprenderán los conceptos básicos, como por ejemplo: datagrama o paquete; los principales protocolos que se encuentran en los diferentes niveles de estos protocolos y los servicios que ofrecen a los usuarios, todo esto explicado con definiciones y figuras.

CAPITULO 1

INTRODUCCION

CAPITULO 1: INTRODUCCION

El protocolo *TCP/IP* son varios protocolos en uno, de los cuales, dos son los mas importantes para los protocolos de *Internet*:

TCP: Protocolo de Transmisión.

IP: Protocolo de Internet.

Estos protocolos fueron desarrollados inicialmente en 1973 por el informatico estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la *ARPA* (Agencia de Programas Avanzados de Investigación) del Departamento Estadounidense de Defensa, de la cual se hizo una red dedicada exclusivamente a aspectos militares (*MILNET*).

Internet comenzó siendo una red informática de *ARPA* (conocida como *ARPANET*) que conectaba redes de ordenadores de varias universidades y laboratorios de investigación en los Estados Unidos.

Para comunicar las redes, se desarrollaron varios protocolos el *TCP* y el *IP*, posteriormente estos protocolos se fueron englobando en el conjunto del protocolo *TCP/IP*. La *ARPANET* dejo de funcionar oficialmente en 1990.

Lo que hoy se conoce como la World Wibe Web (Red Mundial) se desarrolló en 1989 por el informatico británico Timothy Berners-Lee para la *CERN* (Consejo Europeo de Investigación Nuclear).

El protocolo *TCP/IP* , va enlazado con la Internet y se difundió mundialmente.

Algunos de los motivos por lo cual se popularizo son:

- Independencia del fabricante.
- Soporta múltiples tecnologías.
- Puede funcionar en maquinas de cualquier tamaño.
- Respeta los protocolos de cada red individual.

TCP/IP es el protocolo más utilizado por todos los ordenadores conectados a *Internet*, de manera que todos estos pueden comunicarse entre sí. En la *Internet* se encuentran conectados toda clase de ordenadores con diferentes hardware y software (sistema operativo), que en muchos casos son incompatibles (como por ejemplo *MAC y PC*), sin importar los medios y formas de conexión. Es precisamente aquí donde se encuentra una de las grandes ventajas del protocolo *TCP/IP*, el cual se encargará de que sea posible la comunicación.

Como cualquier máquina de la red puede comunicarse con otra distinta, esta conectividad permite enlazar redes físicamente independientes en una red virtual llamada *Internet*. Las máquinas en Internet son denominadas "*hosts*" o nodos, las cuales conectan universidades, agencias gubernamentales, empresas privadas y computadoras personales; teniendo acceso a una gran variedad de información. como: política, comercio, cultura y entretenimiento, solo por mencionar algunos.

CAPITULO 2

PROTOCOLOS TCP/IP

CAPITULO 2: PROTOCOLOS TCP/IP

Los protocolos *TCP/IP* están divididos en 5 niveles funcionales:

APLICACIÓN
TRANSPORTE
INTERNET
RED
FÍSICO

- El nivel *físico* corresponde al hardware. Puede ser cable coaxial, cable par trenzado, cable de fibra óptica o una línea telefónica. *TCP/IP* no considera oficialmente el nivel físico como componente específico de su modelo y tiende a agrupar el nivel físico con el nivel de red.

Los protocolos principales que interactuan en este nivel son:

FTP, SMTP, TELNET	SNMP, X - WINDOWS RPC, NFS
TCP	UDP

ARP (Addres Resolution Protocol): este es un protocolo que se utiliza para convertir las direcciones *IP* en direcciones de la red física, es decir, para poder hacer esta conversión, existe un ordenador para cada módulo *ARP*, que utiliza una Tabla de direcciones. Si no se encuentra dicha dirección en la Tabla, se genera una petición *ARP* para que alguno de los ordenadores de la red reconozca su propia dirección *IP* en la petición ARP y se graba en la Tabla de direcciones *ARP*.

RARP (Reverse Addres Resolution Protocol): este protocolo se utiliza cuando, al producirse el arranque inicial, los ordenadores no conocen su dirección *IP*. Se requiere al menos un servidor *RARP*, es decir, al recibir el paquete, busca en su Tabla *RARP* su dirección *IP* correspondiente a la dirección física inicial indica en el paquete y envían un paquete al ordenador origen con la información.

- El nivel de *red* es la interfaz de la red real. Se van a describir los siguientes protocolos:

SPLI (Serial-Line Internet Protocol): es un protocolo antiguo desarrollado para el entorno *UNIX*.

PPP (Point-to-point Protocol): es un protocolo *SPLI* mejorado con control y recuperación de errores.

- El nivel de *Internet* se encuentran los siguientes protocolos en que se divide el *TCP/IP*.

ICMP (Internet Control Message Protocol) es un protocolo de mantenimiento/gestión de red que ayuda a supervisar.

Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino.

El principal objetivo de *ICMP* es proporcionar la información de error o control entre nodos.

Los mensajes de error de este protocolo normalmente los genera y los procesa *TCP/IP* y no el usuario.

Existen cuatro tipos de mensajes *ICMP*:

- Mensajes de destino no alcanzable.
- Mensajes de control de congestión.
- Mensajes de redireccionamiento.
- Mensajes de tiempo excedido.

IP (Internet Protocol): este protocolo se encarga de seleccionar la trayectoria a seguir por los *datagramas*, es decir, por donde se deben encaminar los *datagramas* salientes pudiendo llevar a cabo tareas de fragmentación y reensamblado.

■ El nivel de *transporte* se encuentran los protocolos siguientes:

TCP (Transmission Control Protocol): es un protocolo orientado a conexión que utiliza los servicios del nivel *Internet*.

UDP (User Datagram Protocol): es un protocolo que se basa en el intercambio de *datagramas*. Este protocolo permite el envío de datagramas a través de la red sin que haya establecido previamente una conexión, ya que el propio *datagrama* incorpora suficiente información de direccionamiento en su *cabecera*.

■ En el nivel de *aplicación* se utilizan todas las aplicaciones conforme al modelo cliente/servidor.

En este nivel se encuentran una gran cantidad de protocolos, aquí se encuentran los protocolos destinados a proporcionar servicios, de los cuales los principales son:

FTP (File Transfer Protocol) es el protocolo más utilizado de todos los protocolos de aplicación y más antiguo, porque se utiliza para transferencia de archivos.

HTTP (HyperText Transport Protocol) es uno de lo protocolos más recientes. Se utiliza para manejar la consulta de hipertexto y el acceso de datos con la *WWW* (World Wide Web).

NFS (Network File System) este protocolo permite la utilización de archivos distribuidos por los programas de la red, es decir, autoriza a los usuarios el acceso a archivos que se encuentran en sistemas remotos.

NTP (Network Time Protocol) este protocolo permite que todos los sistemas sincronicen su hora con un sistema designado como servidor horario.

RPC (Remote Procedure Call) este protocolo permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a *RCP* como si fueran procedimientos locales.

El proceso cliente envía un mensaje al proceso servidor y espera una respuesta. Éste, al recibir la llamada, estudia los procedimientos, obtiene los resultados y los envía al proceso cliente mediante un mensaje de respuesta.

Existen dos tipos de servidores:

- El servidor *iterativo* que recibe una llamada proporciona el servicio y vuelve al estado de espera.

- El servidor *concurrente* que recibe la llamada, contesta al mensaje enviando al cliente un número de puerta, arranca un proceso paralelo para prestar el servicio requerido por el cliente y vuelve al estado de espera. Cuando el servicio paralelo haya finalizado el servicio requerido, acaba su ejecución.

SMTP (Simple Network Management Protocol) este protocolo sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el tráfico de la red.

TELNET: este protocolo estándar del *TCP/IP* es para servicio de terminal remota. *TELNET* permite 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.

Se fundamenta en tres principios:

- El concepto de terminal virtual de red. (*NVT*). Corresponde a la definición de cómo han de ser los datos, caracteres de control y las secuencias de los mandatos que han de circular por la pared para permitir una heterogeneidad de los sistemas.

- La simetría entre terminales y procesos. La comunicación puede ocurrir entre dos terminales, dos procesos o entre una terminal o un proceso.

- Permite que el cliente y el servidor negocien sus opciones. La conexión comienza con una fase de negación de opciones en la que se utilizan cuatro mandatos: WILL, WONT, DO y DONT.

  WILL se envía para mostrar el deseo de comenzar una opción (que se ha de indicar) y se contesta con DO (respuesta positiva) o DONT (respuesta negativa).

  WONT se envía para mostrar el deseo de no comenzar una opción (que se ha de indicar) y se contesta con DONT (mostrando el acuerdo de no utilización).

DO se envía para indicar que comience a utilizar una opción (que se ha de indicar) y se contesta con WILL (respuesta positiva) o WONT (respuesta negativa).

DONT se envía para indicar que no comience a utilizar una opción (que se ha de indicar) y se contesta con WONT (mostrando el acuerdo de no utilización).

TFTP (Trivial File Transfer Protocol) es un protocolo destinado a la transferencia de ficheros pero sin permitir tanta interacción entre cliente y servidor como la que existe en *FTP*.

X-WINDOWS es un protocolo para el manejo de ventanas e interfaces de usuario.

CAPITULO 3

TCP/IP Y EL MODELO OSI

CAPITULO 3: TCP/IP Y EL MODELO OSI

De los niveles del protocolo *TCP/IP* corresponden con los niveles del modelo de referencia *OSI*, siendo que este ultimo tiene dos niveles mas como se ve en la figura la siguiente:

TCP/IP	OSI
	Aplicación
	Presentación
Aplicación	Sesión
Transporte	Transporte
Internet	Red
Red	Enlace de datos
Físico	Físico

También existen correspondencias teóricas entre los protocolos *TCP/IP* y el *modelo OSI*, siendo que este ultimo fue desarrollado posteriormente que el *TCP/IP*.

La arquitectura de *Internet* esta basada en niveles. Esto hace mas fácil implementar nuevos protocolos. La relación del modelo *TCP/IP* con el *modelo OSI* esta en la siguiente figura:

<table>
<tr><td>Aplicación</td><td rowspan="3">TELNET</td><td rowspan="3">FTP</td><td rowspan="3">SNMP</td><td rowspan="3">DNS</td><td rowspan="3">HTTP</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td colspan="5">TCP</td></tr>
<tr><td>Red</td><td colspan="5">IP</td></tr>
<tr><td>Enlace de datos</td><td colspan="3">802</td><td>X.25</td><td>ATM</td></tr>
<tr><td>Física</td><td>Ethernet</td><td colspan="2">Token Ring</td><td colspan="2">WAN</td></tr>
</table>

Sus diferencias más importantes son:

- *El concepto de jerarquía en la relación a los niveles.* Indica que una tarea de comunicaciones se divide en entidades que se pueden comunicar con otras entidades pares en otro sistema. Una entidad dentro de un sistema proporciona servicios a otras entidades, y, a su vez, utiliza los servicios de otras. Estas entidades deben tener una relación jerárquica.

- *La fiabilidad extremo a extremo.* El protocolo IP no es fiable, es decir, no garantiza que los paquetes entregados sean correctos y que conserven la secuencia con que fueron emitidos, ya que se supone que los protocolos de transporte deben garantizarlo.

- *Los servicios no orientados a conexión.* El *protocolo IP* tampoco es orientado a conexión, ya que ésta debe proporcionarse en niveles superiores.

CAPITULO 4

PROTOCOLO IP

CAPITULO 4: PROTOCOLO IP

La tarea de *IP* es llevar los datos (los *paquetes*) de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas *enrutadores*) utilizan *IP* para trasladar los datos.

IP a diferencia del *protocolo X.25*, que está orientado a conexión, es sin conexión. Está basado en la idea de los *datagramas* interred, los cuales son transportados transparentemente, pero no siempre con seguridad, desde el hostal fuente hasta el hostal destinatario, quizás recorriendo varias redes mientras viaja.

El *protocolo IP* trabaja de la siguiente manera; la capa de transporte toma los mensajes y los divide en *datagramas*, de hasta 64K *octetos* cada uno. Cada d*atagrama* se transmite a través de la red interred, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

Un *datagrama IP* consta de una parte de cabecera y una parte de texto. La cabecera tiene una parte fija de 20 octetos y una parte opcional de longitud variable.

El campo *opciones* se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información. Proporciona un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no está presente en el diseño original. También, para permitir que los experimentadores trabajen con nuevas ideas y para evitar, la asignación de bits de cabecera a información que muy rara vez se necesita.

Debido a que la *longitud de la cabecera* no es constante, un campo de la cabecera, *IHL*, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits. El valor mínimo es de 5. Tamaño 4 bit.

El campo *tipo de servicio* le permite al hostal indicarle a la subred el tipo de servicio que desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Para voz digitalizada, por ejemplo, es más importante la entrega rápida que corregir errores de transmisión. En tanto que, para la transferencia de archivos, resulta más importante tener la transmisión fiable que entrega rápida. También, es posible tener algunas otras combinaciones, desde un tráfico rutinario, hasta una anulación instantánea. Tamaño 8 bit.

La *Longitud total* incluye todo lo que se encuentra en el datagrama -tanto la cabecera como los datos. La máxima longitud es de 65 536 octetos(bytes). Tamaño 16 bit.

El campo *identificación* se necesita para permitir que el hostal destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación. Tamaño 16 bits.

Enseguida viene un bit que no se utiliza, y después dos campos de 1 bit. Esta es una orden para que las pasarelas no fragmenten el *datagrama*, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente.

El *desplazamiento de fragmento* indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65 536 octetos, que coinciden con el campo *Longitud total*. Tamaño 16 bits.

El campo *tiempo de vida* es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos. Tamaño 8 bits.

Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitará saber qué hacer con él. El campo *Protocolo* indica, a qué proceso de transporte pertenece el datagrama.

Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. *Tamaño: 8 bit.*

El *código de redundancia de la cabecera* es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del *código de redundancia* de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida. *Tamaño: 16 bit*

La dirección de origen contiene la dirección del *host* que envía el paquete. *Tamaño: 32 bit.*

La Dirección de destino: esta dirección es la del *host* que recibirá la información. Los *routers* o *gateways* intermedios deben conocerla para dirigir correctamente el paquete. *Tamaño: 32 bit.*

CAPITULO 5

PROTOCOLO TCP

CAPITULO 5: PROTOCOLO TCP

Como ya se menciono que el *protocolo IP* mueve los paquetes de datos a granel, el *protocolo TCP* se encarga del flujo y asegura que los datos estén correctos.

Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino. Esto es semejante de como se transmite una conversación telefónica. Una vez que establece una conexión, se reservan algunos circuitos para usted, que no puede emplear en otra llamada.

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

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

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

Una entidad de transporte *TCP* acepta mensajes de longitud grande procedentes de los procesos de usuario, los separa en pedazos que no excedan de 64K octetos y, transmite cada pedazo como si fuera un datagrama separado. La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que *TCP* deberá utilizar temporizadores y retransmitir los datagramas si es necesario. Los *datagramas* que consiguen llegar, pueden hacerlo en desorden; y dependerá de *TCP* el hecho de reensamblarlos en mensajes, con la secuencia correcta.

Cada *octeto* de datos transmitido por *TCP* tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecidos, desde hace tiempo, en el momento en que los números de secuencia den la vuelta. *TCP*, sin embargo, sí se ocupa en forma explícita del problema de los duplicados retardados cuando intenta establecer una conexión, utilizando el protocolo de ida-vuelta-ida para este propósito.

La cabecera mínima de *TCP* es de 20 octetos.

A diferencia de la clase 4 del *modelo OSI*, con la cual se puede comparar a grandes rasgos, *TCP* sólo tiene un formato de cabecera de *TPDU* (llamadas mensajes). Enseguida se analizará minuciosamente campo por campo, esta gran cabecera. Los campos *Puerto fuente y Puerto destino* identifican los puntos terminales de la conexión. Cada hostal deberá decidir por sí mismo cómo asignar sus puertos.

Los campos *número de secuencia y asentimiento en superposición* efectúan sus funciones usuales. Estos tienen una longitud de 32 bits, debido a que cada octeto de datos está numerado en *TCP*.

La *longitud de la cabecera TCP* indica el número de palabra de 32 bits que están contenidas en la cabecera de *TCP*. Esta información es necesaria porque el campo *opciones* tiene una longitud variable, y por lo tanto la cabecera también.

El puntero acelerado se emplea para indicar un desplazamiento en octetos a partir del número de secuencia actual en el que se encuentran datos acelerados. Esta facilidad se brinda en lugar de los mensajes de interrupción. Después de cerrar una conexión, un proceso puede seguir recibiendo datos indefinidamente.

El control de flujo en *TCP* se trata mediante el uso de una *ventana* deslizante de tamaño variable. Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos que se pueden transmitir más allá del octeto aprovado por el campo ventana.

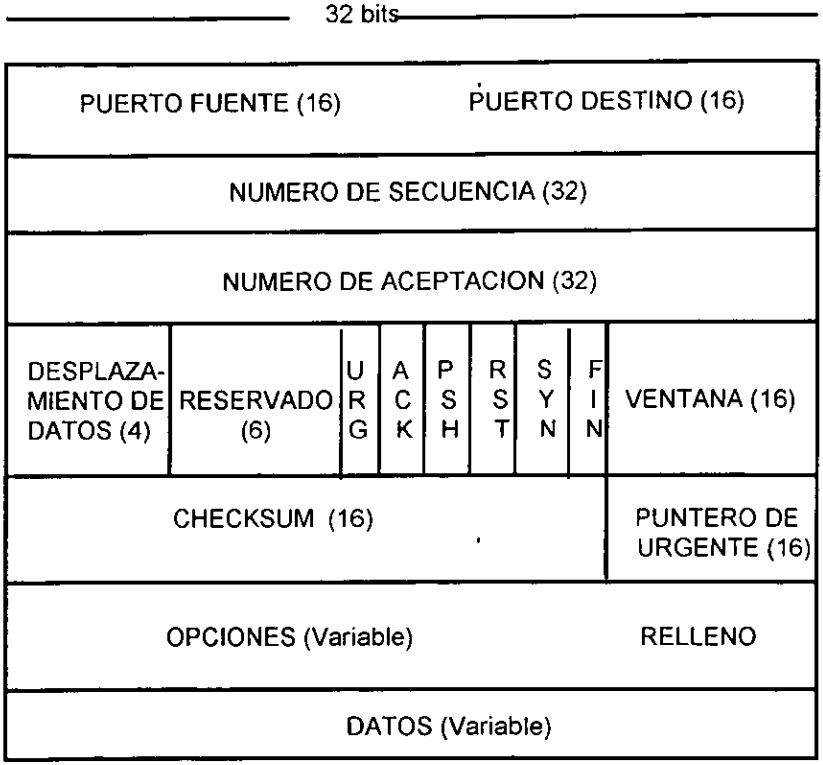
El *código de redundancia* también se brinda como un factor de seguridad extrema. El algoritmo de código de redundancia consiste en sumar simplemente todos los datos, considerados como palabras de 16 bits, y después tomar el complemento a 1 de la suma.

Generalizando TCP es un protocolo orientado a conexión. Esto quiere decir que TCP mantiene información del estado de cada cadena de datos de usuario que circula por él. El término utilizado en este contexto significa también que TCP es responsable de la transferencia de datos entre extremos por la red o redes hasta la aplicación de usuario receptor. TCP debe asegurar que los datos se transmiten y se reciben correctamente por los computadores atravesando las correspondientes redes.

Como TCP es un protocolo orientado a conexión, es responsable de la *transferencia fiable* de cada uno de los caracteres que recibe de la capa superior correspondiente. En consecuencia, utiliza números de secuencia y aceptaciones/rechazos.

El segmento TCP

Las PDU que se intercambian entre dos módulos TCP se denominan *segmentos*. En la siguiente figura se muestra el formato de un segmento.



- El *número de secuencia* se utiliza para la operación de gestión de la conexión. Si dos entidades TCP utilizan el segmento de solicitud de conexión, entonces el número de secuencia especificada el número de *secuencia de envío inicial* que se utilizará para la numeración subsiguiente de los datos de usuario.

- El valor del número de *aceptación* permite aceptar los datos previamente recibidos. Este campo contiene el valor del número de secuencia del siguiente octeto que se espera recibir del transmisor.

- El campo de *desplazamiento de datos* especifica el número de palabras alineadas de 32 bits de que consta la cabecera de TCP. Este campo se utiliza para determinar donde comienza el campo de datos.

- El campo *reservado* está reservado y consta de 6 bits que deben valer cero. Estos bits están reservados para usos futuros.

- Los seis bits indicadores (flags), son bits de control de TCP y se utilizan para especificar ciertos servicios o utilidades que se pueden usar durante la sesión.

    - URG indica que el campo de puntero de urgencia es significativo.
    - ACK indica si el campo de aceptación es significativo.
    - PSH significa que el módulo va a utilizar la función push.
    - RST indica que la conexión se va a iniciar.
    - SYN indica que se van a sincronizar los números de secuencia.
    - FIN indica que el remitente no tiene más datos para enviar.

- El campo *ventana* se pone a una valor que indica cuántos octetos desea aceptar el receptor. Este valor se establece teniendo en cuenta el valor del campo de aceptación. La ventana se establece sumando los valores del campo de ventana y del campo de número de aceptación.

- El campo de *checksum* contiene el complemento a 1 de 16 bits del complemento a 1 de la suma de todas las palabras de 16 bits del segmento, incluyendo la cabecera y el texto. Determina si el segmento procedente del transmisor ha llegado libre de errores.

- El campo *puntero de urgente* es que el objeto de este puntero es identificar el octeto de datos al que siguen datos urgentes, solo se indica el lugar donde empiezan los datos urgentes, no lo que hay que hacer con ellos.
- El campo de *opciones* está concebido para futuras mejoras de TCP.
- El campo de *relleno* asegura que la cabecera TCP ocupa un múltiplo par de 32 bits.

CAPITULO 6

DIRECCIONAMIENTO IP

CAPITULO 6: DIRECCIONAMIENTO IP

Las direcciones IP permiten que el envío de datos entre ordenadores se haga de forma eficaz, de modo parecido a como se utilizan los números de teléfono en las llamadas telefónicas.

El *protocolo IP* identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bit que debe ser único para cada *host*, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en *Internet* se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- *Clase A:* son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los *hosts* que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. Existien algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".

- *Clase B*: estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254. Los dos últimos bytes de la dirección constituyen el identificador del *host* permitiendo, por consiguiente, un número máximo de 64 516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de ordenadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".

- *Clase C*: en este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el *host*, lo que permite que se conecten un máximo de 254 ordenadores en cada red. Estas direcciones permiten un menor número de *host* que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

- *Clase D*: se reserva todas las direcciones para multidestino (multicasting), 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*: se utiliza únicamente con fines 'experimentales. Las direcciones estarán comprendidas entre 240.0.0.0 y 247.255.255.255.

Tabla de direcciones IP principales de internet.

Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1..126	1 byte	3 byte	126	16 387 064
B	128..191	2 byte	2 byte	16 256	64 516
C	192..223	3 byte	1 byte	2 064 512	254

En la clasificación de direcciones se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales.

También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

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

El número 255 tiene también un significado especial, puesto que se reserva para el *broadcast*.

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

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

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

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (*subnets*).

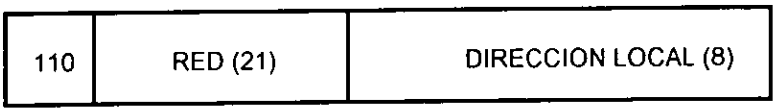
La estructura de Direcciones IP

En la figura siguiente se muestra la estructura de una dirección IP. Su formato es DIRECCION IP = DIRECCION DE RED + DIRECCION DE COMPUTADOR.

CLASE A

CLASE B

CLASE C

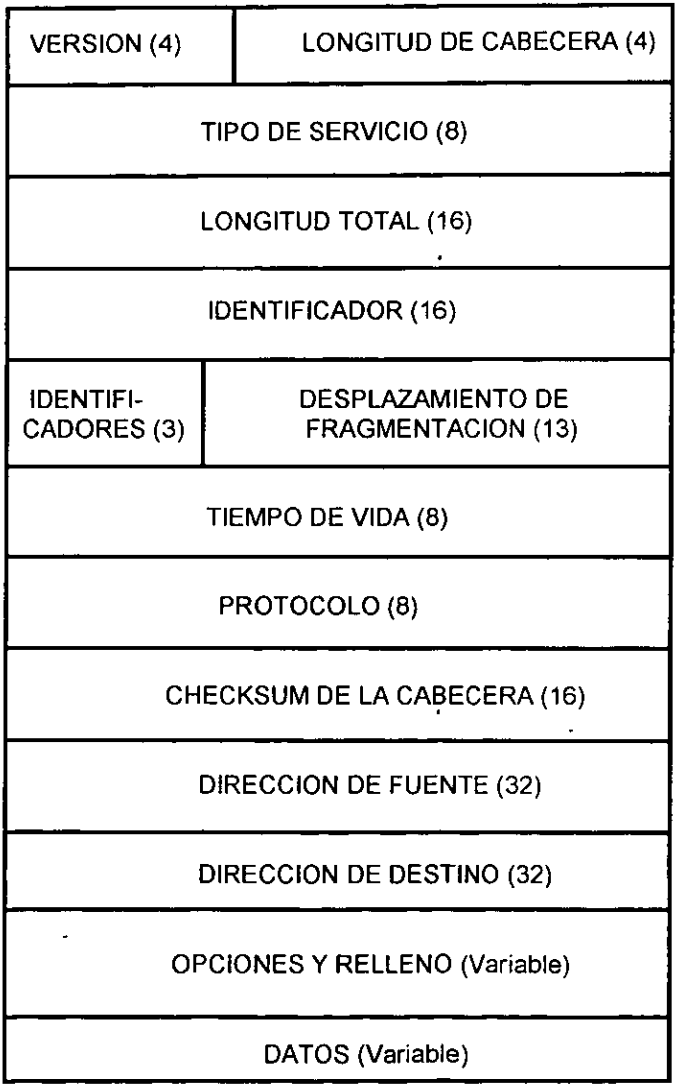


CLASE D

CLASE E

El datagrama de IP

En el análisis de IP consiste en examinar los campos del datagrama de IP (PDU) que se muestra en la siguiente figura:



- El campo de *versión* identifica la versión de IP en uso. La mayoría de los protocolos tienen este campo debido a que algunos nodos pueden no utilizar la última versión del protocolo disponible.

- El campo de *longitud de cabecera* contiene cuatro bits con el valor de la longitud de la cabecera del datagrama. La longitud se mide en palabras de 32 bits. Normalmente una cabecera tiene 20 octetos. Por lo tanto, el valor del campo de longitud habitualmente es de 5.

- El campo de *tipo de servicio* se puede utilizar para identificar varias funciones de Internet. El retardo de tránsito, el caudal efectivo, la precedencia y la fiabilidad se pueden solicitar utilizando este campo.

- El campo de *longitud total* especifica la longitud total del datagrama de IP. Se mide en octetos e incluye la longitud de la cabecera y de los datos. IP resta el valor del campo de longitud de cabecera del valor del campo de longitud total para obtener el tamaño del campo de datos. La longitud máxima de un datagrama es de 65 535 octetos (2^{16}). Las pasarelas que dan servicio a datagramas de IP deben aceptar cualquier datagrama que soporte el tamaño máximo de las PDU de las redes conectadas. Adicionalmente, todas las pasarelas deben aceptar datagramas de 576 octetos lo longitud total.

- El protocolo IP utiliza tres campos de datos en la cabecera que sirven para controlar la fragmentación y ensamblado del datagrama. Son *identificador*, los *indicadores* y el *desplazamiento de fragmentación*.

  El campo de identificador se utiliza para identificar todos los fragmentos de un datagrama original . Se utiliza junto con la dirección fuente del computador receptor para identificar el fragmento.

El campo de identificadores contiene bits que indican si el datagrama se puede fragmentar y, si se puede fragmentar uno de los bits que si se puede poner a 1 para indicar el último fragmento del datagrama original.

El campo de desplazamiento de fragmentación contiene un valor que especifica la posición relativa del fragmento en el datagrama orifinal. Su valor se inicializa a cero y se v aponiendo al valor apropiado a medida que la pasarela fragmenta los datos. El valor se mide en unidades de 8 octetos.

- El parámetro de *tiempo de vida* se utiliza para medir el tiempo que un datagrama lleva en la Internet. Es muy similar al campo de tiempo de vida de los protocolos de redes no orientadas a conexión. Todas la pasarelas de la Internet deben observar este campo y descartarlo si el valor es cero. Las pasarelas deben también decrementar el valor de ese campo en todos los datagramas que procesan. Cuando un datagrama pasa por una pasarela "salta" el valor de ese campo que se decrementa en una unidad. Algunas realizaciones de IP utilizan un contador de tiempo para este campo y decrementan su valor en unidades de 1 segundo.

- El campo de *protocolo* se utiliza para identificar el siguinete protocolo en la estructura de niveles por encima de IP que va a recibir el datagrama en el computador de destino. Los grupos de normalización Internet han ideado un sistema de numeración que identifica a los protocolos de nivel superior más ampliamente utilizados.

- El *checksum de la cabecara* se utiliza para *detectar* distorsiones en la cabecera. No se realizan comprobaciones en la cadena de datos de usuario. Algunos sectores críticos a IP indican que si se detectan errores en los datos de usuario, las pasarelas podrían al menos notificar al computador remitente que hay problemas.

- El datagrama de IP lleva dos direcciones: *dirección de fuente* y *dirección de destino*, no se modifican durante toda la vida del datagrama.

- El campo de *opciones* se emplea para identificar diversos servicios adicionales. El campo de opciones no se utiliza en todos los datagramas. La mayoría de los esquemas utilizan este campo para gestión de la red y diagnósticos.

- El campo de *relleno* se puede utilizar para asegurar de que la cabecera del datagrama se alinea exactamente con una división de intervalo de 32 bits.

- El campo de *datos* contiene los datos de usuario. IP estipula que la combinación de los campos de cabecera y de datos no puede sobrepasar los 65 535 octetos.

CAPITULO 7

SIMILITUDES Y DIFERENCIAS ENTRE EL NIVEL 4 DEL MODELO OSI Y TCP

CAPITULO 7: SIMILITUDES Y DIFERENCIAS ENTRE EL NIVEL 4 DEL MODELO OSI Y TCP

El protocolo de transporte de nivel 4 del *modelo OSI* (se le llama *TP4*), y *TCP* tienen numerosas similitudes, pero también algunas diferencias.

Son iguales en:

- Los dos protocolos están diseñados para proporcionar un servicio de transporte seguro, orientado a conexión y de extremo a extremo, sobre una red insegura, que puede perder, dañar, almacenar y duplicar paquetes.

- Los dos deben enfrentarse a los peores problemas como sería el caso de una subred que pudiera almacenar una secuencia válida de paquetes y más tarde volviera a entregarlos.

- Los dos protocolos también son semejantes por el hecho de que los dos tienen una fase de establecimiento de conexión, una fase de transferencia de datos y después una fase de liberación de la conexión.

En particular, tanto TP4 como TCP utilizan la comunicación ida-vuelta-ida para eliminar las dificultades potenciales ocasionadas por paquetes antiguos que aparecieran súbitamente y pudiesen causar problemas.

- Primero, TP4 utiliza nueve tipos diferentes de *TPDU*, en tanto que *TCP* sólo tiene uno. Esta diferencia trae como resultado que *TCP* sea más sencillo, pero al mismo tiempo también necesita una cabecera más grande, porque todos los campos deben estar presentes en todas las *TPDU*. El mínimo tamaño de la cabecera *TCP* es de 20 octetos; el mínimo tamaño de la cabecera TP4 es de 5 octetos. Los dos protocolos permiten campos opcionales, que pueden incrementar el tamaño de las cabeceras por encima del mínimo permitido.

- Una segunda diferencia es con respecto a lo que sucede cuando los dos procesos, en forma simultánea, intentan establecer conexiones entre los mismos dos *TSAP* (una colisión de conexiones). Con *TP4* se establecen dos conexiones duplex independientes; en tanto que con *TCP*, una conexión se identifica mediante un par de *TSAP*, por lo que solamente se establece una conexión.

- Una tercera diferencia es con respecto al formato de direcciones que se utiliza. TP4 no especifica el formato exacto de una dirección TSAP; mientras que TCP utiliza números de 32 bits.

- La cuarta diferenciaes que TP4 tiene un mecanismo de extremo abierto, bastante elaborado, para una negociación a tres bandas sobre la calidad de servicio. Esta negociación incluye al proceso que hace la llamada, al proceso que es llamado y al mismo servicio de transporte. Se pueden especificar muchos parámetros, y pueden proporcionarse los valores: deseado y mínimo aceptable. A diferencia de esto, *TCP* no tiene ningún campo de calidad de servicio, sino que el servicio subyacente *IP* tiene un campo de 8 bits, el cual permite que se haga una relación a partir de un número limitado de combinaciones de velocidad y seguridad.

- Una quinta diferencia es que *TP4* permite que los datos del usuario sean transportados en la TPDU, pero *TCP* no permite que los datos del usuario aparezcan en la *TPDU* inicial. El dato inicial (ejemplo, una contraseña), podría ser necesario para decidir si se debe, o no, establecer una conexión. Con *TCP* no es posible hacer que el establecimiento dependa de los datos del usuario.

- La sexta esta en que el modelo *TCP* es de un flujo continuo de octetos, sin que haya ningún límite explícito entre mensajes.

- La séptima diferencia se ocupa de cómo son tratados los datos importantes que necesitan de un procesamiento. *TP4* tiene dos flujos de mensajes independientes, los datos normales y los acelerados multiplexados de manera conjunta. En cualquier instante únicamente un mensaje acelerado puede estar activo. *TCP* utiliza el campo Acelerado para indicar que cierta cantidad de octetos.

- La octava diferencia es la ausencia del concepto de superposición en *TP4* y su presencia en *TCP*.

- La novena diferencia se relaciona con la forma como se trata el control de flujo. *TP4* puede utilizar un esquema de crédito, pero también se puede basar en el esquema de ventana de la capa de red para regular el flujo. *TCP* siempre utiliza un mecanismo de control de flujo explícito con el tamaño de la ventana especificado en cada *TPDU*.

- La décima diferencia se relaciona en que ambos protocolos, el receptor tiene la capacidad de reducir la ventana en forma voluntaria. En *TCP* no hay ninguna solución para este problema; en tanto en *TP4* éste se resuelve por medio del número de subsecuencia que está incluido en la contracción.

- La onceava diferencia que existente entre los dos protocolos, consiste en la manera como se liberan las conexiones. *TP4* utiliza una desconexión abrupta en la que una serie de *TPDU* de datos pueden ser seguidos directamente por una TPDU. Si las *TPDU* de datos se llegaran a perder, el protocolo no los podría recuperar y la información, al final se perdería. *TCP* utiliza una comunicación de ida-vuelta-ida para evitar la pérdida de datos en el momento de la desconexión.

Diferencias entre el protocolo TP4 del modelo OSI y TCP se muestran en la siguiente figura:

Caracteristicas	OSI TP4	TCP
Número de tipos de TPDU	9	1
Fallo de Conexión	2 conexiones	1 conexión
Formato de direcciones	No está definido	32 bits
Calidad de servicio	Extremo abierto	Opciones específicas
Datos del usuario en CR	Permitido	No permitido
Flujo	Mensajes	Octetos
Datos importantes	Acelerados	Acelerados
Superposición	No	Sí
Control de flujo explícito	Algunas veces	Siempre
Número de subsecuencia	Permitidos	No Permitido
Liberación	Abrupta	Ordenada

CAPITULO 8

LA NUEVA VERSION DE IP (IPng)

CAPITULO 8: LA NUEVA VERSIÓN DE IP (IPng)

La nueva versión del *protocolo IP* recibe el nombre de IPv6, aunque es también conocido comúnmente como IPng (*Internet Protocol Next Generation*). El número de versión de este protocolo es el 6 frente a la antigua versión. Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión antigua no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo.

IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Ethernet, etc.)

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual.

Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

Formato de la cabecera.

El tamaño de la cabecera que el protocolo IPv6 añade a los datos es de 320 bit, el doble que en la versión antigua. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunós campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera los *routers* no tienen que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión.

El formato completo de la cabecera sin las extensiones es el siguiente:

- *Versión:* número de versión del *protocolo IP*, que en este caso contendrá el valor 6. Tamaño: 4 bit.

- *Prioridad:* contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. Tamaño: 4 bit.

- *Etiqueta de flujo:* campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los *routers* que lo soporten. Tamaño: 24 bit.

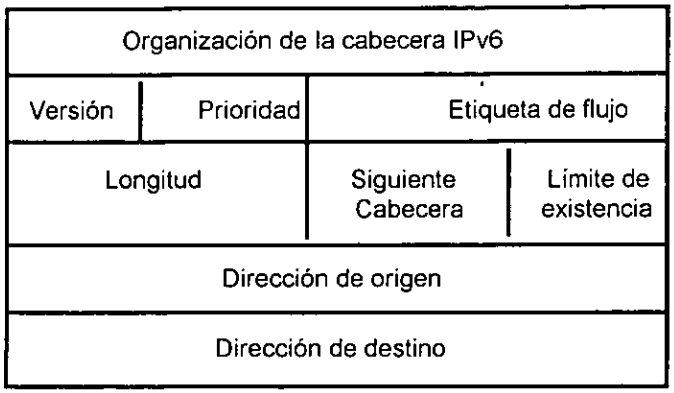
- *Longitud:* es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. Tamaño: 16 bit.

- *Siguiente cabecera:* se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. Tamaño: 8 bit.

- *Límite de existencia:* Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. Tamaño:8 bit.

- *Dirección de origen:* El número de dirección del *host* que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. Tamaño: 128 bit.

- *Dirección de destino:* Número de dirección de destino, aunque puede no coincidir con la dirección del *host* final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. Tamaño: 128 bit.



Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para *routing* extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

Direcciones en la versión 6

El sistema de direcciones es uno de los cambios más importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 bit (cuatro veces mayor).

El número de direcciones diferentes que pueden utilizarse con 128 bits es enorme. Teóricamente serían 2128 direcciones posibles, siempre que no apliquemos algún formato u organización a estas direcciones. Este número es extremadamente alto, pudiendo llegar a soportar más de 665.000 *trillones* de direcciones distintas por cada *metro cuadrado* de la superficie del planeta Tierra. Según diversas fuentes consultadas, estos números una vez organizados de forma práctica y jerárquica quedarían reducidos en el peor de los casos a 1.564 direcciones por cada metro cuadrado, y siendo optimistas se podrían alcanzar entre los tres y cuatro trillones.

Existen tres tipos básicos de direcciones IPng según se utilicen para identificar a un interfaz en concreto o a un grupo de interfaces. Los bits de mayor peso de los que componen la dirección IPng son los que permiten distinguir el tipo de dirección, empleándose un número variable de bits para cada caso. Estos tres tipos de direcciones son:

- **Direcciones *unicast:*** Son las direcciones dirigidas a un único interfaz de la red. Las direcciones *unicast* que se encuentran definidas actualmente están divididas en varios grupos. Dentro de este tipo de direcciones se encuentra también un formato especial que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP.

- **Direcciones *anycast:*** Identifican a un conjunto de interfaces de la red. El paquete se enviará a un interfaz cualquiera de las que forman parte del conjunto. Estas direcciones son en realidad direcciones *unicast* que se encuentran asignadas a varios interfaces, los cuales necesitan ser configurados de manera especial. El formato es el mismo que el de las direcciones *unicast*.

- **Direcciones *multicast:*** Este tipo de direcciones identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente.

CONCLUSIONES

CONCLUSIONES

Como todos los protocolos TCP/IP están englobados en uno solo, no se puede pensar un uno de ellos separadamente, ya que los cinco niveles en su conjunto sirven para lo mas importante: transmitir y recibir información eficazmente de un lugar del mundo a otro.

Los protocolos TCP/IP son de gran importancia para el desarrollo de las redes de comunicación, principalmente para la Internet. Gracias a los protocolos TCP/IP es posible conectar redes de distintas tecnologías, sin importar su hardware o software, logrando con ello una verdadera globalización mundial en lo que se refiere a la información.

De una forma mas particular se dice que el protocolo IP es el canal a seguir, en donde se lleva la información de un computador a otro. En cambio el protocolo TCP
es el que se encarga y asegura de que esta información llegue a su destino; que en su conjunto es lo que hace funcionar a la Internet.

El fin de los protocolos TCP/IP es tener una transmisión y recepción de información rápida y eficaz por la red; aunque hoy en día no todas las personas cuentan con una computadora con módem, sigue siendo de fácil acceso la Internet (cafés Internet principalmente).

Muy pronto será común tener Internet en casa, como lo es el teléfono o la televisión.

GLOSARIO

802

Norma IEEE 802.

ARP

Address Resolution Protocol "protocolo de resolución de direcciones". Es un protocolo que se usa para averiguar la dirección del enlace correspondiente a la dirección IP.

ARPA

Agencia de Programas Avanzados de Investigación del departamento de defensa de E.U.A.

ARPANET

Fue desarrollada en 1969 por ARPA, para conseguir una red, que propicio el desarrollo de la conmutación de paquetes y del protocolo TCP/IP. Desapareció en 1990. Es el antecesor de la Internet.

ATM

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

Broadcast

Es un sistema de entrega que proporciona la copia de un paquete dado a todos los anfitriones conectados para la difusión del paquete.

CERN

Consejo Europeo de Investigación Nuclear (siglas en francés).

Checksum

"Suma de verificación". Es un número entero calculado a partir de una secuencia de octetos que son tratados como enteros en una suma para calcular su

valor total. Muchos protocolos TCP/IP utilizan una suma de verificación de 16 bits.

Datagrama

Es un paquete individual de datos que es enviado al ordenador receptor sin ninguna información que lo relacione con ningún otro posible paquete enviado.

Dirección

Localización de memoria en la RAM asociada con cada máquina determinada, identificador numérico o nombre simbólico que especifica la ubicación de una máquina o dispositivo en particular en una red, y un medio para identificar una red, subred o nodo completos dentro de una red.

NDS

Domain Name System "sistema de nombres de dominio". Sistema automatizado que sirve para traducir nombres de computadoras a direcciones IP equivalentes.

Ethernet

Es un tipo particular de red de área local que usa una tipología de canal compartido. En este tipo de red los ordenadores pueden utilizar el protocolo TCP/IP.

FTP

File Transfer Protocol "protocolo de transferencia de archivos". Es una aplicación de Internet que permite transferir archivos de un ordenador a otro.

Hipertexto

Es una de las características de las páginas de Internet. Se le denomina así a la capacidad de saltar de un documento a otro por medio de imágenes o en el propio texto con solo pulsar la tecla del ratón sobre él, lo que permite "navegar" ya sea dentro de una Web o hacia otras.

Host

Cualquier sistema de computadora de usuario final que se conecta a una red.

HTTP

Hyper Taxt Transport Protocol "protocolo de transporte de hipertexto". Es un protocolo diseñado para responder a los requerimientos de los navegadores.

ICMP

Internet Control Message Protocol "protocolo de control de mensajes de Internet". Sirve para integrar el protocolo de Internet que resuelve errores y controla los mensajes.

IEEE

Instituto de Ingenieros Eléctricos y Electrónicos. Organización profesional de ingenieros que propone y aprueba estándares.

Interfaz

Punto compartido entre dos aplicaciones de software o dos dispositivos de hardware.

Internet

Conjunto de redes conectadas entre si que cubren a todo el mundo. Internet es el término específico para una interred más general o grupo de redes, para una conexión virtual.

ISO

International Organization for Standardization "organización internacional de normalización". La organización mejor conocida por haber propuesto el modelo de referencia de los 7 niveles de la conectividad de datos.

IP

Internet Protocol "protocolo de Internet". Es el protocolo de nivel de red usado en Internet. Mediante este protocolo, cualquier paquete puede viajar a través de las distintas redes de Internet hasta llegar a su destino final.

MILNET

Military Network "red militar". Originalmente parte de ARPANET, está se separó en 1984.

Multicast

"Multidifusión". Técnica que permite que copias de un solo paquete se transfieran a un subconjunto seleccionado de todos los destinos posibles.

NFS

National Science Foundation "fundación científica nacional". Dependencia gubernamental de E.U.A. que inició algunas de las investigaciones y desarrollos de Internet.

OSI

Open System Interconnect "interconexión de sistemas abiertos". El modelo OSI es una serie de protocolos normalizados por la Organización Internacional para la Normalización (ISO).

Paquete

En una red los datos transmitidos por un ordenador son divididos en conjuntos de caracteres independientes. Cada paquete viaja por la red independientemente de los demás hasta llegar a su destino.

PDC

Primary Domain Crontroller "controlador del dominio primario". Es un servidor de dominio que contiene la copia maestra de la seguridad y las cuentas de los usuarios para autentificar sus accesos.

PDU

Unidad de Datos de Protocolo

PPP

Point to Point Protocol "protocolo punto a punto". Es un protocolo utilizado para acceder a Internet mediante una línea telefónica y un módem. Se acceden a Internet con plenos derechos a través de una simple línea telefónica.

Protocolo

Es un conjunto de normas que indican cómo deben actuar los ordenadores para comunicarse entre sí.

RARP

Reverse Address Resolution Protocol "protocolo de resolución de direcciones invertido". Es un protocolo para una maquina sin disco utiliza al arrancar para encontrar su dirección IP.

Router

"Ruteador". Computadora que se conecta a dos o más redes y envía paquetes de una red a otra.

RPC

Remote Procedure Call "llamadas a procedimientos remotos". Se utilizan para áreas remotas.

SMTP

Simple Mail Transfer Protocol "protocolo de transferencia de correo simple". Es una aplicación para el correo electrónico.

SNMP

Simple Network Management Protocol "protocolo de administración de red simple". Es un protocolo de aplicación para el control de la red.

TCP

Transmission Control Protocol "protocolo de control de transmisión". Protocolo del nivel de transporte que forma parte del grupo de protocolos TCP/IP y proporciona un flujo de datos confiables basado en conexión.

TELNEL

Es un protocolo para el manejo de ventanas e interfaces de usuario.

TFTP

Trivial File Transfer Protocol "protocolo de transporte de archivo trivial". Es un protocolo simple de transferencia de ficheros que usa UDP.

Token Ring

Protocolo para red de nivel inferior basado en conexión que emplean el método de paso de señales para controlar el tráfico de datos.

TP4

Protocolo diseñado por ISO, similar al TCP.

TPDU

Unidad de Datos de Protocolo de Transporte.

TSAP

Punto de Acceso de Servicios de Transporte.

UDP

User Datagram Protocol "protocolo de datagrama de uso". Es el protocolo sobre el que funcionan ciertos servicios de Internet. Se utiliza cuando se necesita transmitir voz o video.

WAN

Red de área amplia. Es una red formada por nodos conectados en una área geográfica extensa.

WWW

World Wibe Web "red mundial. Sistema de hipermedios usado en Internet en el que una página de información puede contener texto, imágenes, fragmentos de audio o video y referencias a otras paginas.

X.25

Es un protocolo de transmisión de red de paquetes ISO utilizado en muchas redes de área extensa.

X-Windows

Es un protocolo para el manejo de ventanas e interfaces de usuario.

BIBLIOGRAFIA

■ DOMINE TCP/IP
José Luis Raya Cabrera y Víctor Rodrigo Raya
Editorial RA-MA

■ REDES DE COMPUTADORES, PROTOCOLOS, NORMAS E INTERFACES
Uyless Black
2da. Edición
Editorial Computec

■ REDES GLOBALES DE INFORMACION CON INTERNET Y TCP/IP
Douglas E. Comer
Tercera edición
Editorial PRENTICE-HALL

■ REDES LOCALES
José Felix Rábago
Editorial Anaya Multimedia

■ REDES DE COMPUTADORES, INTERNET E INTERREDES
Douglas E. Comer
Editorial PRENTICE-HALL

■ APRENDIENDO TCP/IP EN 14 DIAS
Tim Parker
Editorial PRENTICE-HALL

■ EDICION ESPECIAL: REDES CON MICROSOFT TCP/IP
Drew Heywood
Editorial PRENTICE-HALL