59

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUATITLAN

"TELEFONÍA DIGITAL Y RDSI.
PRINCIPIOS DE FUNCIONAMIENTO DEL
PROTOCOLO TCP/IP"

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A :

SAÚL MACHORRO LÓPEZ

ASESOR: ING. VICENTE MAGAÑA GONZÁLEZ

CUATITLAN IZCALLI, EDO. DE MÉXICO 2001

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:

Telefonía Digital y RDSI
"Principios de Funcionamiento del Protocolo TCP/IP"

que presenta él pasante: Machorro López Saúl
con número de cuenta: 9361678-6 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 3 de Mayo de 2001.

MODULO	PROFESOR	FIRMA
I	Ing. José Luis Rivera López	
III	Ing. Blanca de la Peña Valencia	
IV	Ing. Vicente Magaña González	

AGRADECIMIENTOS

Gracias a Dios que me ayudo y me dio la fuerza para poder estudiar y llegar a la culminación de un ciclo más en mi vida, al ver realizado el sueño de terminar mi carrera.

Gracias a Mi Padre y a Mi madre que invirtieron su tiempo para formarme y darme educación. Y por saberme encaminar a través del camino del éxito personal y profesional, al enseñarme a confiar en Dios y guiarme en sus enseñanzas.

Gracias a Blanca que con su paciencia y dedicación a sabido llevarme a una vida Feliz y plena.

PROLOGO

La familia de protocolos TCP/IP (*Transmisión Control Protocol/Internet Protocol*), es la base de la Internet actual, así como la base de muchas redes privadas de computadoras. La familia de protocolos TCP/IP, que no es tan solo TCP e IP, permiten a las computadoras de una red comunicarse entre ellas.

TCP/IP se desarrollo inicialmente para permitir que los sitios conectados a *ARPANET* se comunicasen entre sí. Los sitios de *ARPANET* utilizaban computadoras de distintos fabricantes y con distintos sistemas operativos; lo único que tenían en común entre sí era el protocolo de comunicación TCP/IP.

Este trabajo pretende dar los principios básicos del funcionamiento del protocolo TCP/IP, sin profundizar demasiado en su estudio. Lo que se pretende es dar la base para un estudio formal del conjunto de protocolos. En este trabajo se dará mayor importancia a la capa de Internet y Transporte del modelo TCP/IP, por considerar que estas dos capas son las más representativas del funcionamiento de este protocolo.

La capa de Interfaz de red y su funcionamiento, se toca de manera breve en el primer capítulo de este trabajo; la capa de aplicación y sus protocolos se mencionaran en el último capítulo de esta tesina.

Este trabajo se encuentra dividido en cinco capítulos a lo largo de los cuales se darán los *Principios de Funcionamiento del protocolo TCP/IP.*

En el primer capítulo de este trabajo se vera una breve reseña desde los inicios del protocolo TCP/IP con la red de *ARPANET* hasta el nacimiento de lo que hoy conocemos como la red de *INTERNET.*

Se verá una introducción al modelo OSI que sirve de referencia para varios protocolos, así como una comparación entre el modelo OSI y el modelo utilizado por el protocolo TCP/IP.

En el segundo capítulo se describe el funcionamiento del protocolo IP, dando una introducción básica a los protocolos principales de la capa de Internet como el protocolo *ICMP (Internet Control Message Protocol)* y el Protocolo *IP (Internet Protocol)*. En este capítulo se describen las principales funciones y servicios que proporcionan estos dos protocolos a todo el conjunto TCP/IP.

En el tercer capítulo se trata el formato de la dirección IP, en su forma decimal y binaria; así como las clases de direcciones IP que existen actualmente. Por otro lado se dará el concepto básico de lo que es una subred dentro del contexto de una red IP.

En el capítulo cuatro se tratarán los principales protocolos de la capa de transporte como el *UDP (User Datagram Protocol)* y el *TCP (Transmission Control Protocol)*, en el cual se verán algunas de sus principales características y servicios, como por ejemplo, los estados de una conexión TCP y el establecimiento de una conexión a través del *Protocolo de Control de Transmisión.*

En el capítulo cinco se mencionará de forma breve algunos de los principales protocolos de aplicación y su función.

PRINCIPIOS DE FUNCIONAMIENTO DEL PROTOCOLO TCP/IP

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN AL TCP/IP

1.1 HISTORIA Y CARACTERÍSTICAS DE TCP/IP

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP). fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA. siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPAnet) que conectaba redes de ordenadores de varias universidades y laboratorios de investigación en Estados Unidos.

Durante los años setenta creció el número de sitios conectados a ARPANET, inicialmente de manera lineal, pero a finales de los 70's el crecimiento se hizo exponencial.

Se necesitaba algo mejor, y a finales de los 70's empezó a ver la luz lo que ahora conocemos como TCP/IP. La RFC 760, que describe el Protocolo de Internet, se publicó el 1 de enero de 1980. Posteriormente fue sustituida por la RFC 791, publicada en septiembre de 1981, junto con una RFC que describía TCP (RFC 793). La RFC 768, describiendo el Protocolo de Datagramas de Usuario, UDP (*User Datagram Protocol)*, se había editado un año antes.

Estas RFC definen el núcleo de la familia de protocolos de TCP/IP que aún se utilizan hoy. Aunque han cambiado algunos detalles y se ha añadido alguna funcionalidad, estos protocolos han superado el paso del tiempo y continúan sirviendo a su propósito. El esquema de direccionamiento de TCP, con un esquema de dirección de IP de 32 bits, ha demostrado ser no adecuado para la Internet de hoy, pero nadie de los años setenta hubiese predicho en lo que se ha convertido Internet.

En 1980, se incluyo en el UNIX 4.2 de BERKELEY, y fue el protocolo militar estándar en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se popularizo bastante, y su destino va unido al de Internet. ARPANET dejo de funcionar oficialmente en 1990.

Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en maquinas de cualquier tamaño

- Estándar de EEUU desde 1983

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Conectividad Universal a través de la red
- Reconocimientos de extremo a extremo
- Protocolos estandarizados

1.2 TCP/IP Y EL MODELO OSI

1.2.1 Modelo OSI.

El desarrollo de ARPANET se inició en un lugar académico. Para entonces no tenía mucho interés comercial. Durante los años setenta, la necesidad de más redes abiertas era tema de conversación en la industria de la computación. Como las redes eran homogéneas, normalmente no se podía comunicar computadoras de distintos fabricantes.

En 1977, ISO empezó el desarrollo de un modelo de referencia detallado OSI. La idea del modelo OSI era permitir el desarrollo de software que consiguiese un sistema abierto; un sistema que permaneciese abierto a los demás con el objeto de poderse intercambiar información con otros. La suposición era que un sistema abierto usaría los estándares aplicables, y por tanto, sería capaz de Interoperar.

El modelo OSI es un estándar muy débil en el que las definiciones y mucha terminología resultan vagas. Era deliberado asegurar que el modelo no imponía ninguna restricción a un implementador para usar ninguna técnica ó terminología existente. En su lugar se pretendía promocionar el desarrollo de protocolos que permitiesen la interconexión de sistemas heterogéneos. El modelo OSI también funciona como un modelo de referencia que permite comparar otros protocolos y estándares.

El modelo OSI arranca con la premisa de que la comunicación entre dos computadoras es suficientemente compleja como para no considerarla como una sola entidad. En lugar de ello, las funciones que constituyen el proceso de comunicación debería dividirse en una serie de niveles, también denominados capas, separados, donde cada nivel sucesivo se

construye sobre el nivel inferior usando las funciones asignadas a dicho nivel. El funcionamiento concreto interno de cada uno de los niveles, se dejaba para los implementadores. La clave era estandarizar las funciones de cada uno de los niveles y las interfaces entre ellos.

El modelo OSI de ISO consta de siete niveles, como se muestra en la siguiente figura 1.1.

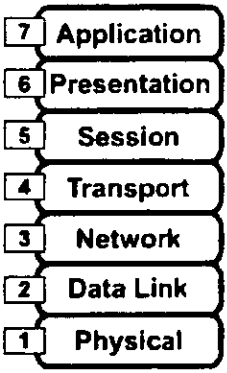

Figura 1. 1 Capas del modelo OSI

En este modelo la aplicación y el usuario están en la parte superior, mientras en la parte inferior, esta el medio físico de comunicación. Las funciones de los niveles en orden ascendente son las siguientes:

Físico (Physical): Pone un flujo de bits en el medio físico. Este nivel típicamente se implementa en hardware.

Enlace de datos (Data Link): Define el concepto de paquete, (una trama) y permite a una computadora enviar tramas a otra computadora conectada en el mismo cable. Típicamente se implementa con una mezcla de harware y software.

Red (Network): Permite que dos sistemas se envíen paquetes de datos a través de una interconexión de redes usando los niveles inferiores. Este nivel está implementado en software. Este nivel es no fiable ya que las tramas que se envían por la red se pueden perder, se pueden enrutar mal o se pueden corromper. Los niveles superiores son los responsables de la fiabilidad.

Transporte (Transport): Permite la transmisión fiable de datos a través de una red. Utiliza la comunicación entre extremos que proporciona el nivel de red y añade fiabilidad.

Sesión (Session): Añade el concepto de sesiones entre dos sistemas, donde las computadoras en una sesión guardan información sobre el estado de la sesión y más tarde usan esa información para futuros procesamientos.

Presentación (Presentation): Se encarga de la traducción de datos entre distintos formatos, según se necesite (por ejemplo entre ASCII) separando por tanto, los formatos del cable de los formatos que ve la aplicación.

Aplicación (Application): Este nivel es donde se encuentran las aplicaciones y los usuarios. Las aplicaciones usan los otros seis niveles para implementar una función de negocio utilizando la red subyacente.

1.2.2 Modelo TCP/IP

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

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

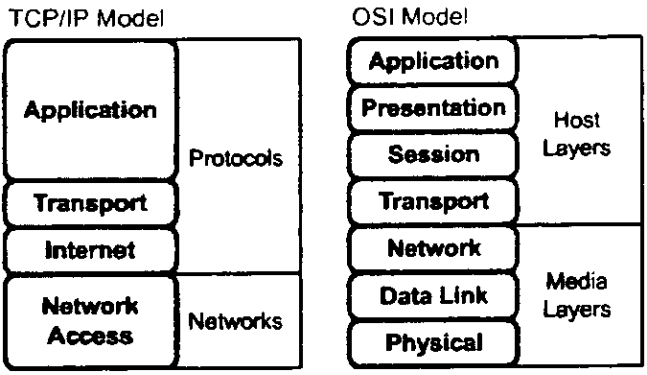

Figura 1. 2 Comparación del Modelo TCP/IP y el Modelo OSI

Aplicación: Corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).

Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

Físico: El Nivel de Red Física corresponde al hardware, su definición eléctrico mecánica, puede ser un cable coaxial, par trenzado c fibra óptica. El protocolo Principal de esta capa es ARP (Address Resolution Protocol): Se encarga de convertir las direcciones IP en direcciones de red Física.

Red : Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

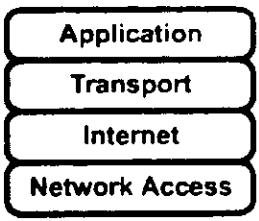

Figura 1. 3 Modelo TCP/IP

C A P Í T U L O 2

FUNCIONAMIENTO DEL PROTOCOLO TCP/IP

2.1 CAPA DE INTERNET

2.1.1 Introducción

La capa de Internet se superpone a la red física creando un servicio de Red Virtual independiente de aquella. No es fiable y no es orientado a conexión. Esta capa se encarga del direccionamiento y enrutamiento de los datos hasta la estación receptora.

En este nivel se encuentran dos protocolos principales: *ICMP (Internet Control Message Protocol)* cuya función principal es proporcionar información de error y control entre nodos, a través de mensajes generados por TCP/IP y no por el usuario, hay 4 tipos de mensajes ICMP: Mensajes de destino no alcanzable, mensaje de control de congestión, mensaje de redireccionamiento, mensaje de tiempo excedido.

El segundo protocolo es *IP (Internet Protocol)*, el cual se encarga de seleccionar la ruta a seguir por los datagramas y de su enrutamiento a través de la red de datos. Se caracteriza por ser un protocolo orientado a no conexión, es decir, que no existe acuerdo entre los nodos antes de enviar la información. Y no se crea ni se mantiene una conexión lógica en el Nivel de Internet.

2.1.2 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. 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, y no el usuario.

2.1.2.1 Formato del mensaje ICMP

Cada Mensaje ICMP esta compuesto por los siguientes campos:

- **Tipo**. Campo de 1 byte que indica el tipo de mensaje de ICMP. En la tabla 3.1 se muestran los mensajes más comunes.

- **Código.** Campo de 1 byte que indica un mensaje especifico dentro de un tipo de mensaje de ICMP. este campo código se establece a 0. La combinación de tipo y código determina un mensaje concreto ICMP.
- **Checksum.** Campo de 2 bytes para una suma de comprobación de 16 bits para el mensaje de ICMP.
- **Otras variables.** Datos opcionales para cada tipo de ICMP.

Tipos de mensaje ICMP

Tipo	Tipo de Mensaje
0	Respuesta de Eco
3	Destino Inalcanzable
4	Origen saturado
5	Redirección (cambiar ruta)
8	Solicitud de eco
11	Tiempo excedido para un datagrama
12	Problema de parámetros en un datagrama
13	Solicitud de fecha y hora
14	Respuesta de fecha y hora
17	Solicitud de mascara de dirección
18	Respuesta de mascara de dirección

Tabla 2.1 Tipos de Mensajes ICMP

2.1.2.2 Solicitud de Eco.

Un *Host* puede comprobar si otro *Host* es operativo mandando una solicitud de eco. El receptor de la solicitud la devuelve a su origen. Esta aplicación recibe el nombre de *Ping*. Esta utilidad encapsula la solicitud de eco del ICMP (tipo 8) en un datagrama IP y lo manda a la dirección IP.

El receptor de la solicitud de eco intercambia las direcciones del datagrama IP, cambia el código a 0 y lo devuelve al origen.

2.1.2.3 Informes de Destinos Inalcanzables.

Si un *Gateways* no puede enviar un datagrama a la dirección de destino, este manda un mensaje de error ICMP al origen. El valor del campo tipo es 3, y el tipo de error viene dado por el campo código. Tabla 2.2

Códigos de Destino Inalcanzable

Código	Descripción
0	Red no alcanzable
1	Host no alcanzable
2	Protocolo no alcanzable
3	Puerto no alcanzable
4	Necesaria fragmentación con la opción DF
5	Fallo de la ruta de origen
6	Red de Destino desconocida
7	Host de Destino desconocido
8	Fallo del Host de Origen
9	Red prohibida administrativamente
10	Host prohibido administrativamente
11	Tipo de servicio de Red no alcanzable
12	Tipo de servicio de Host no alcanzable

Tabla 2.2 Códigos de destino Inalcanzable

2.2 Introducción a IP

IP comprende el nivel de INTERNET del modelo TCP/IP y proporciona la funcionalidad de Interconexión, que hace posible la interconexión a gran escala como Internet. IP permanece desde que se formalizo en 1981 y se continuará usando en Internet durante años. Sólo recientemente se han tratado algunas dificultades de IP en una nueva versión IPv6.

2.2.1 Servicios IP

IP ofrece los siguientes servicios a los protocolos de niveles superiores:

- **Protocolo de Interconexión (Internetworking protocol).** IP es un protocolo de interconexión, también conocido como protocolo enrutable. La cabecera de IP contiene la información necesaria para el enrutamiento de un paquete, incluyendo

las direcciones de origen y destino. Una dirección IP consta de dos componentes: una dirección de red y una dirección de nodo. La entrega entre redes o enrutamiento es posible gracias a la existencia de una dirección de red de destino. IP permite la creación de conjunto de redes IP, es decir, dos o más redes interconectadas mediante enrutadores IP.

- **Múltiples protocolos cliente:** IP es un transporte entre redes para los protocolos de niveles superiores. IP puede transportar diferentes protocolos de los niveles superiores, pero cada paquete de IP sólo puede contener datos de un solo protocolo de nivel superior a la vez. Ejemplos de protocolos de nivel superior son el Protocolo de Mensajes de Control de Internet, ICMP (Internet Control Managment Protocol), Protocolo de Control de Transmisión, TCP (Transmission Control Protocol), y el Protocolo de Datagramas de Usuario, UDP (User Datagram Protocol).
- **Entrega de datagramas.** IP es un protocolo de datagramas que proporciona un servicio de entrega no fiable y sin conexión a los protocolos de niveles superiores. Sin conexión significa que no existe acuerdo entre los nodos de IP antes de enviar los datos y que nos se crea ni mantiene una conexión lógica en el Nivel de Internet.
- **Independencia del nivel de interfaz de red.** En el Nivel de Internet, IP es independiente del nivel físico de OSI como el cableado, la señalización y la velocidad. También es independiente del nivel de Enlace de Datos del modelo OSI, como el esquema de control de acceso al medio y el tamaño máximo de trama.
- **Fragmentación y reensamblado.** Para admitir el máximo tamaño de trama de distintas tecnologías de interfaz de red, IP permite la fragmentación de los datos cuando se envían por un enlace cuya MTU es menor que el tamaño de un datagrama.
- **Extensible mediante las opciones de IP.** Cuando se requieren funciones que no están disponibles, se pueden usar las opciones IP: Estas opciones se añaden a la cabecera estándar para proporcionar la funcionalidad como la capacidad de especificar una ruta que debe de seguir un datagrama a través de una Inter-red.
- **Tecnología de datagramas por conmutación de paquetes.** IP es un ejemplo de una tecnología de datagramas por conmutación de paquetes: cada paquete es un datagrama, un mensaje sin secuencia ni asentamiento que se reenvía por los

conmutadores de la red de conmutación usando un esquema de direcciones con significado global. En el caso de IP, cada conmutador de la red es un enrutador de IP, el direccionamiento con significado global es la dirección del destino IP. Esta dirección se examina en cada enrutador. El enrutador toma una dirección de enrutamiento independiente y reenvía el paquete. Como cada enrutador decide de manera independiente donde reenviar el paquete, la ruta de un paquete desde un Nodo uno hasta un Nodo dos no es necesariamente la misma ruta que desde el Nodo dos hasta el Nodo uno. Además, como cada paquete se conmuta de forma separada, cada uno puede llevar una ruta distinta desde el origen hasta el destino; y debido a distintos retardos en el trayecto, cada paquete puede llegar en un orden distinto al que fue enviado.

2.2.2 Datagrama de IP

Un datagrama de IP consta de una cabecera de IP y unos datos de IP, como se muestra en la figura 2.1.

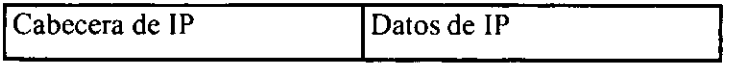

Figura 2.1 Un Datagrama de IP consta de Cabecera de IP y unos datos de IP

- **Cabecera de IP.** La cabecera de IP es de tamaño variable entre 20 y 60 bytes, en incremento de 4 bytes. Proporciona soporte para enrutamiento, identificación de datos, indicación del tamaño de la cabecera de IP, fragmentación y opciones.
- **Datos de IP.** Los Datos de IP son de tamaño variable, desde los 8 bytes (un datagrama de IP de 68 bytes con una cabecera de IP de 60 bytes) hasta los 65,515 bytes (un datagrama de IP de 65,535 bytes con una cabecera de IP de 20 bytes).

2.2.3 Cabecera de IP

En la figura 2.2 se muestra la estructura de la cabecera IP. En la siguiente sección se tratan los campos de la cabecera.

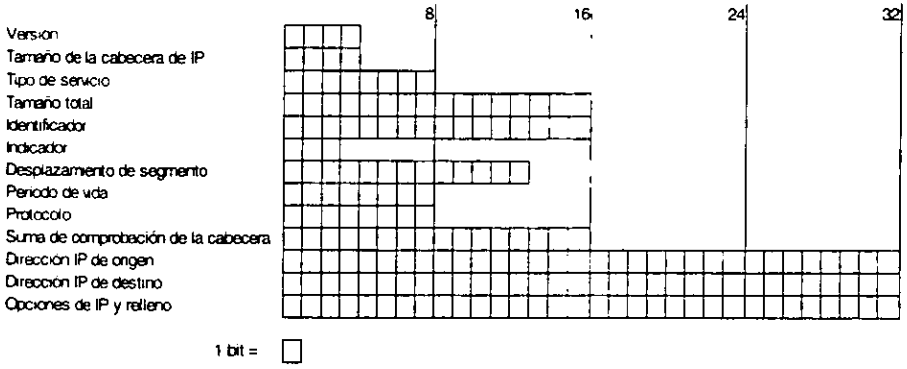

Figura 2.2 Formato de la cabecera IP

Versión

El campo versión tiene 4 bits de tamaño y se usa para indicar la versión de la cabecera IP. Un campo de 4 bits puede tener valores desde 0 hasta 15. La versión estándar que se usa hoy en redes corporativas e Internet es la versión 4, IPv4. La siguiente versión de IP es la versión 6, IPv6. El resto de los valores del campo no se utilizan.

Tamaño de la cabecera

El campo tamaño de la cabecera (Header length) tiene 4 bits de tamaño y se usa para indicar el tamaño de la cabecera de IP. El número máximo que se puede representar es de 15, por tanto este campo no es un contador de bytes. Indica el número de palabras de 32 bits, bloques de 4 bytes, de la cabecera de IP.

Al usar un contador de bloque de 4 bits indica que el tamaño de la cabecera de IP siempre ha de ser múltiplo de 4 bytes. Si hay opciones de IP que extiendan la cabecera, deben hacerlo en incremento de 4 bytes, se debe usar un relleno para que la cabecera siempre este en la frontera de 4 bytes.

Tipo de servicio

El campo tipo de servicio, TOS (Type Of Service), tiene 8 bits de tamaño y se usa para indicar la calidad de servicio con que los enrutadores del conjunto de redes deben enviar

ese datagrama. El TOS tiene subcampos e indicadores para indicar características de procedencia deseada, retardo, rendimiento, fiabilidad y coste.

Tamaño Total

El campo tamaño total tiene 2 bytes y se usa para indicar el tamaño del datagrama de IP (Cabecera de IP y datos de IP) en bytes. Con los 16 bits, el tamaño máximo que se puede indicar es de 65.535 bytes. Para los datagramas de tamaño máximo, el tamaño total es el mismo que la MTU de IP para dicha tecnología del nivel de interfaz de red.

Con el tamaño de cabecera y el tamaño total se puede determinar el tamaño de los datos: Tamaño de los datos IP(bytes) = Tamaño total(bytes) – 4 * Tamaño de la cabecera(Palabras de 32 bits).

Identificación

El campo identificación tiene 2 bytes de tamaño y se usa para identificar un paquete de IP concreto enviado entre un nodo emisor y un nodo de destino. El host emisor fija el valor del campo identificación que se incrementa en sucesivos datagramas de IP. Este campo se usa para identificar fragmentos de un datagrama de IP original.

Indicadores

El campo indicadores consta de 3 bits y contiene los indicadores para la fragmentación. Un indicador se usa para indicar si el datagrama de IP es elegible para fragmentación y el resto indica si siguen más fragmentos o no.

Desplazamiento de fragmento

El campo desplazamiento de fragmento tiene 13 bits de tamaño y se usa para indicar el desplazamiento donde este fragmento empieza relativo a los datos originales de IP.

Período de vida

El campo período de vida tiene 1 byte de tamaño y se usa para indicar cuantos enlaces puede atravesar este datagrama de IP antes que un enrutador lo descarte. El campo período de vida TTL (Time To Live) se diseño como un contador de tiempo para indicar el número de segundos que el datagrama podía estar vivo en la Internet.

Protocolo

El campo protocolo tiene 1 byte y se utiliza para indicar el protocolo de nivel superior que contiene los datos de IP. El campo protocolo es una indicación explicita del protocolo cliente.

Suma de comprobación de cabecera

El campo suma de comprobación de cabecera tiene 2 bytes y realiza una comprobación de integridad en el nivel de bits sólo de la cabecera de IP. Los datos de IP no se incluyen.

Dirección IP de origen

El campo dirección de origen tiene 4 bytes y contiene la dirección IP del hosts emisor a no ser que un traductor de direcciones de red NAT (Network Address Translator), este traduciendo el datagrama de IP. Se utiliza NAT para traducir entre direcciones privadas y públicas cuando se conectan a Internet.

Dirección de destino

El campo dirección de destino tiene 4 bytes y contiene la dirección de IP del host de destino.

Opciones y relleno

A la cabecera de IP se le pueden añadir opciones y relleno, pero se debe hacer en incrementos de 4 bytes de manera que al tamaño de la cabecera de IP se puede indicar en el campo tamaño de cabecera.

CAPÍTULO 3

DIRECCIONAMIENTO IP

3 DIRECCIONAMIENTO IP

3.1 Introducción

Para entender bien TCP/IP, hay que comprender completamente uno de sus protocolos más importantes: el protocolo IP (*Internet Protocol*). Este protocolo es el bloque de interconexión de redes del resto de protocolos del Nivel de Internet y superiores.
Una dirección IP es una dirección lógica de 32 bits de uno de los siguientes tipos:

- **Unicast.** Una dirección de IP se designa a una única interfaz de red conectada al conjunto de redes IP. Las direcciones unicast de IP se usan en las comunicaciones de uno a uno.
- **Difusión.** Una dirección de difusión de IP se designa para su procesado por todos los nodos de IP del mismo segmento de red. Las direcciones de difusión de IP se usan en la comunicación de uno a todos.
- **Multidifusión.** Una dirección de multidifusión de IP es una dirección en la que uno o más nodos pueden estar escuchando en el mismo o distinto segmento de red. Una dirección de multidifusión se usa en una comunicación de uno a muchos.

3.2 Direcciones de IP

Las direcciones de IP son cantidades de 32 bits que se dividen desde el bit de mayor orden hasta el bit de menor orden, en cuatro cantidades de 8 bits llamadas bytes. Las direcciones de IP se suelen escribir como 4 bytes separados en decimal y separados por un punto (.). Es lo que se conoce como notación decimal con punto.
Por ejemplo, la siguiente dirección de IP:

00001010 00000001 11110001 01000011

Cada byte se convierte a números en base 10 y se separan por puntos:

10.1.241.67

Una dirección IP generalizada se indica como w.x.y.z .

Dirección IP unicast

La dirección de IP unicast es una dirección del conjunto de redes para los nodos de IP que constan de un **Identificador de Red (*ID de Red*)** y de un ***Identificador de host (ID de host.)***

El ID de red, o dirección de red, identifica a todos los nodos ubicados en la misma red lógica. En la mayoría de los casos una red lógica es la misma que el segmento de red físico cuya frontera esta definida por los enrutadores de IP. El ID de red debe de ser único para interred.

El ID de host, o dirección de host, identifica a un nodo dentro de una red. Un nodo es un enrutador o un host, un sistema con interfaz que no es de un enrutador, como una estación de trabajo, un servidor u otro sistema que utilice TCP/IP. El ID de host debe ser el único en cada segmento de red.

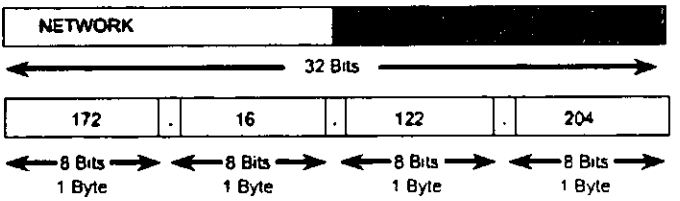

Figura 3.1 Formato de la dirección IP

3.3 Clases de direcciones de IP

Direcciones de Clase A

Las direcciones de clase A se diseñaron para redes con un gran número de hosts. El bit de mayor orden se establece a 0. Los primeros 8 bits definen el ID de red, los 24 bits restantes definen el ID de hosts.

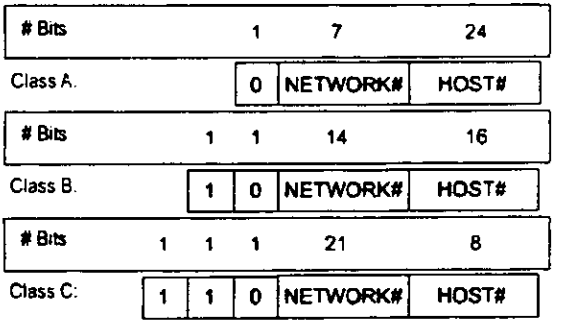

Figura 3.2 Bits utilizados para las clases de direcciones

Direcciones de clase B

Las direcciones de clase B se diseñaron para redes de tamaño moderado con un número moderado de hosts. Los dos bits de mayor orden se establecen a 10. Los primeros 16 bits definen el ID de red y los 16 restantes el ID de host.

Direcciones de clase C

Las direcciones de Clase C se diseñaron para redes pequeñas con un pequeño número de hosts. Los tres bits de mayor peso se establecen a 110. Los primeros 24 bits, definen el ID de red y los 8 restantes el ID de host.

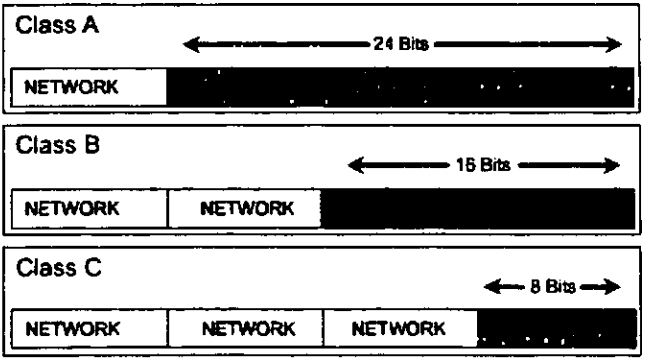

Figura 3. 3 Clases de Direcciones IP

3.3.1 Clases adicionales de direcciones

Clase D

Las direcciones de clase D son direcciones de IP de multidifusión. Los 4 bits de mayor orden se establecen a 1110. Los 28 bits restantes se usan para direcciones de multidifusión individuales.

Clase E

Las direcciones de clase E son direcciones experimentales. Reservadas para usos futuros. Los 5 bits de mayor peso se establecen al valor 11110.

Clase de Dirección	Primer ID de red	Último ID de red	Número de redes
Clase A	1.0.0.0	126.0.0.0	126
Clase B	128.0.0.0	191.255.0.0	16,384
Clase C	192.0.0.0	223.255.255.0	2,097,152

Tabla 3.1 Rangos de las clases de direcciones de Red

Clase de Dirección	Primer ID de Host	Último ID de Host	Número de Host
Clase A	w.0.0.1	w.255.255.254	16,777,214
Clase B	ex.0..1	w.x.255.254	65,534
Clase C	w.x.y.1	w.x.y.254	254

Tabla 3. 2 Rangos de Clases de Direcciones de ID de Host

3.4 Máscara de subred

Con la creación de subredes, un hosts o un enrutador ya no pueden suponer el ID de red y el Id de host de la clase de direcciones de IP. Los nodos necesitan una configuración adicional para distinguir la parte de ID de red de la parte de ID de host de la dirección IP.

La RFC 950 define el uso de una máscara de 4 bytes para identificar que bits de una dirección de IP pertenecen a un ID de red y cuales pertenecen al ID de host. Esta máscara de bits, llamada máscara de subred o máscara de dirección, se define de la siguiente forma:

Si la posición de bit corresponde a un bit en el ID de red, se pone este bit a 1

Si la posición de bit corresponde a un bit en el ID de host, se pone este bit a 0.

Desde la publicación de la RFC 950, los nodos TCP/IP requieren para su configuración una mascara de subred. La longitud de la máscara de subred es de 32 bits.

Clase de dirección	Bits para la mascara de Subred	Mascara de subred
Clase A	11111111 00000000 0000000 00000000	255.0.0.0
Clase B	11111111 11111111 00000000 00000000	255.255.0.0
Clase C	11111111 11111111 11111111 00000000	255.255.255.0

Tabla 3. 3 Notación decimal de la máscara de subred

3.5 Subredes

El incremento en el uso de redes de datos provoco pequeños problemas que no fueron visualizados al aparecer TCP/IP como por ejemplo:

- Se requiere de mucho trabajo administrativo para manejar las direcciones de red
- Las tablas de ruteo se hacen cada vez más grandes.
- El espacio para las direcciones se acaba eventualmente.

La solución a este problema fue, que dos o más redes pequeñas compartan una misma dirección IP, por medio de la utilización de subredes ***(Subnetting)*** y las mascaras de subred. Una subred es un segmento físico en un ambiente TCP/IP, el cual usa direcciones IP derivadas de un ID de red único.

Dividir una red en un conjunto de subredes requiere que cada segmento use un ID de red diferente, o ***ID de subred.*** Un único segmento de subred es creado al dividir los bits del ID de Host, de una dirección IP, en dos partes. Una parte es usada para identificar un segmento de red como único, y la otra parte es usada para identificar al Host.

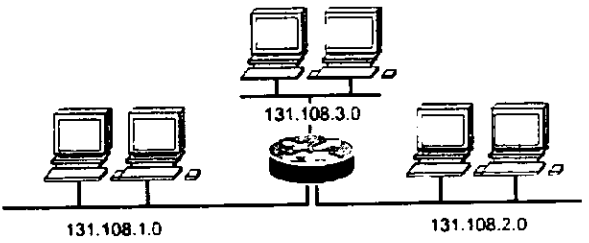

Figura 3. 4 Ejemplo de Subredes

La creación de subredes se diseña para hacer un uso más eficiente de un espacio de direcciones fijo. Un espacio de direcciones fijo es un ID de red de IP. Los bits de red son fijos y los bits de Host son variables. Con la creación de subredes, los bits de ID de Host se pueden utilizar para expresar una combinación de un ID de subred y un ID de Host dentro de una subred y, por tanto una mejor utilización de los bits de Host

CAPÍTULO 4

CAPA DE TRANSPORTE

4. CAPA DE TRANSPORTE

4.1 Introducción

En el Nivel de Transporte existen dos protocolos que usan normalmente los protocolos del nivel de aplicación para el transporte de datos: TCP y el Protocolo de Datagramas de Usuario (UDP). TCP es el protocolo de Nivel de Transporte que proporciona un servicio de envío fiable extremo a extremo, así como un método para transportar datos encapsulados con TCP a un protocolo del nivel de aplicación.

4.2 Protocolo UDP (User Datagram Protocol)

El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP en el sentido de que no es fiable y no esta orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS. Una dirección IP sirve para dirigir el datagrama hacia una maquina en particular, y el número de puerto de destino en la cabecera UDP, se utiliza para dirigir el datagrama UDP a un proceso especifico localizado en la cabecera IP. La cabecera UDP también contiene un número de puerto origen que permite al proceso recibido conocer como responder al datagrama.
El datagrama UDP contiene cuatro campos, que son Número del Puerto de Origen, Número del Puerto de Destino, Longitud del mensaje y Checksum.

Números de Puerto de Origen y Destino

Estos números, junto con las direcciones IP definen el punto final de la comunicación. El número del puerto de origen, puede tener valor cero si no se usa. El número del puerto de destino solo tiene sentido en el contexto de un datagrama UDP y en una dirección IP en particular.
El número de puerto de origen es un campo de 16 bits. El puerto de destino tiene la misma longitud.

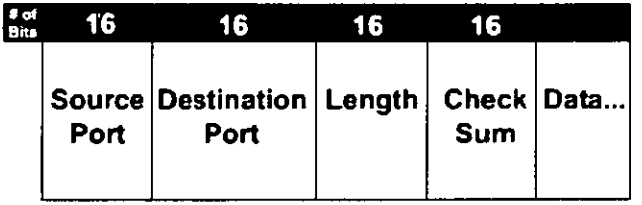

Figura 4. 1 Formato de la Cabecera UDP

Longitud del Mensaje

Este campo tiene una longitud de 16 bits y contiene el número total de octetos que forman el datagrama, incluida la cabecera.

Checksum

El uso del *checksum* es opcional, y este campo debe ponerse a cero si no es utilizado. Mientras que el *checksum* del datagrama IP sólo tiene en cuenta la cabecera del mensaje, el UDP tiene su propio *checksum* para garantizar la integridad de los datos. La longitud de este campo es de 16 bits, y esta formado por la suma de los campos del UDP, y algunos campos del IP.

Para incluir los campos del IP, se construye una pseudo cabecera UDP. Esta pseudo cabecera de 12 octetos se utiliza únicamente a efectos de calcular la suma. (tabla 4.1)

Octeto +0	Octeto +1	Octeto +2	Octeto +3
7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0
Dirección IP de Origen			
Dirección IP de Destino			
Cero	Protocol ID	Longitud	
Puerto Origen		Puerto Destino	
Longitud del Mensaje		Checksum	
Datos UDP			
Datos UDP	Cero		

Tabla 4. 1 Pseudo cabecera UDP

4.3 Introducción a TCP

TCP es un protocolo del nivel de transporte completo que proporciona un servicio de transferencia fiable de datos y un modelo para trasladar datos encapsulados con TCP a un protocolo del nivel de aplicación. TCP tiene las siguientes características:

- **Orientado a conexión.** Antes de transferir los datos, los procesos de nivel de aplicación deben negociar formalmente una conexión de TCP usando el proceso de establecimiento de conexión de TCP. Las conexiones de TCP se cierran formalmente usando el proceso de terminación de conexión de TCP.
- **Full dúplex.** Para cada extremo de TCP, la conexión consta de dos enlaces lógicos: uno de salida y otro de entrada. Con la tecnología apropiada del nivel de interfaz de red los datos pueden fluir hacia fuera por la salida y entrar por el de entrada simultáneamente. La cabecera TCP contiene tanto el número de secuencia de los datos de salida como asentamientos de los datos de entrada.
- **Fiable.** Los datos que se envían por una conexión de TCP se secuencian y se espera una aceptación positiva del receptor. Si no recibe una aceptación, el segmento se

retransmite. En el receptor, los segmentos duplicados se descartan y los segmentos que llegan fuera de secuencia se colocan en su posición dentro de la secuencia. Siempre se usa una suma de comprobación de TCP para verificar la integridad del nivel de bit del segmento TCP.

- **Flujo de bytes.** Para TCP los datos se envían por los enlaces lógicos de entrada y de salida son como un flujo continuo de bytes. El número de secuencia y el número de asentamiento de cada cabecera de TCP se definen en fronteras de bytes TCP.
- **Control de flujo en el extremo emisor y en el extremo receptor.** Para evitar el envío de muchos datos a la vez y congestionar a los enrutadores de un conjunto de redes de IP, TCP implementa control de flujo del extremo emisor que gradualmente regula la cantidad de datos que se envían a la vez. Para evitar que el emisor envíe datos que el receptor no puede guardar en su búfer, TCP implementa control de flujo en el extremo receptor que indica la cantidad de espacio libre en el búfer receptor.
- **Segmentación de datos del nivel de aplicación.** TCP segmentará los datos obtenidos del proceso del nivel de aplicación para que casen con un datagrama de IP para su envío por el enlace del nivel de interfaz de red. Los extremos ajustan el tamaño máximo de segmento mediante el descubrimiento de la unidad máxima de transmisión de la ruta (PMTU).
- **Envío uno a uno.** Las conexiones de TCP son un circuito punto a punto lógico entre dos protocolos del nivel de aplicación. TCP no proporciona un servicio de envío de uno a muchos.

TCP se usa normalmente cuando el protocolo del nivel de aplicación requiere un servicio de transferencia de datos fiable y tal servicio no lo ofrece el propio protocolo del nivel de aplicación.

4.4 Interfaces TCP

Existen dos tipos de interfaces entre la conexión TCP y los otros programas.

El primero es utilizar la pila de los programas de la capa de red. Como en esta capa solo esta el protocolo IP, la interfase lo determina este protocolo. El segundo tipo es la interfaz del programa de usuario. Esta interfase puede variar según el sistema operativo, pero en general tiene las siguientes características.

La interfase envuelve el programa de usuario llamando a una rutina que introduce entradas en una estructura de datos llamada el bloque de control de transmisión (TCB). Las entradas se realizan inicialmente en la pila de hardware y transferidas al TCB por medio de una rutina de sistema. Estas entradas permiten al TCP asociar un usuario con una conexión particular, de modo que pueda aceptar comandos de un usuario y mandarlos a otro usuario en la otra parte de la conexión. TCP utiliza unos identificadores únicos para cada parte de la conexión. Esto se utiliza para recordar la asociación entre dos usuarios. Al usuario se le asigna un nombre de conexión para utilizarlo en futuras entradas del TCB. Los identificadores para cada extremo de la conexión se llaman *sockets*. El socket local se construye concatenando la dirección IP de origen y el número de puerto de origen. El socket remoto se obtiene concatenando la dirección IP de destino y el número de puerto de destino.

El par de sockets de una conexión forman un único número en Internet. El UDP tiene los mismos sockets, pero no los recuerda. Esta es la diferencia entre un protocolo orientado a conexión y otro a no conexión. A continuación se explican los comandos más usuales:

- **Open:** Inicia una conexión o comienza a escuchar un socket. El usuario tiene un nombre de conexión local que actúa como un puntero dentro del TCB.
- **Send:** El comando Send manda datos del buffer especificado.
- **Receive:** El comando Receive es un mensaje de error si el nombre local proporcionado no es utilizado antes con el comando Open.
- **Close:** El comando Close hace que se cierre una conexión. Se produce un error si la conexión especificada no ha sido abierta, o si no se tiene autorización para cerrar la conexión.
- **Status:** El comando Status solo tiene una variable asociada, que es el nombre de la conexión.
- **Abort:** El comando Abort hace que todos los comandos Send y Receive asociados al nombre de la conexión local se interrumpan. La entrada del usuario del TCB se

elimina y se envía un mensaje especial de reinicio a la entidad del otro lado de la conexión.

El TCP recuerda el estado de cada conexión por medio del TCB. Cuando se abre una conexión, se efectúa una entrada única en el TCB. Un nombre de conexión se le asigna al usuario para activar los comandos de la conexión. Cuando se cierra una conexión se elimina su entrada del TCB.

4.4.1 Control de Flujo

El protocolo TCP puede controlar la cantidad de datos que debe enviar mediante el campo Window. Este campo indica el número máximo de octetos que pueden ser recibidos. El receptor de un segmento con el campo window a cero, no puede enviar mensajes al emisor, excepto mensajes de prueba. Un mensaje de prueba es un mensaje de un solo octeto que se utiliza para detectar redes o hosts inalcanzables.

4.5 Formato de la cabecera TCP.

El segmento TCP consiste en una cabecera y datos. A continuación se describen los campos del segmento TCP.

- **Número de puerto del Origen / destino (*Source/Destination Port* Numbers):** Este campo tiene una longitud de 16 bits, y contiene información del puerto de destino de la conexión TCP y el puerto origen.
- **Números de Secuencia (Secuence Numbers):** Campo de 4 bytes que indica el número de secuencia del flujo de bytes de salida del primer byte del segmento. El campo Número de secuencia se pone siempre, aunque no haya datos en el segmento. En este caso este campo se establece al número del siguiente byte del flujo de salida.

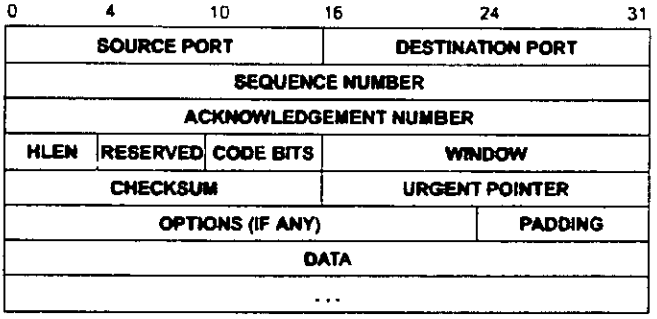

Figura 4. 2 Formato de la cabecera TCP

- **Longitud de la cabecera (Header Length):**Este campo tiene una longitud de 4 bits y contiene un entero igual al número de octetos que forman la cabecera TCP dividido por cuatro.
- **Código de Bits (Code bits):**El motivo y contenido del segmento TCP lo indica este campo. Este campo tiene una longitud de seis bits.

1. Bit URG (bit +5)*:*Este bit identifica datos urgentes.
2. Bit ACK (bit +4):Cuando este bit se pone a 1, el campo reconocimiento es valido.
3. Bit PSH (Bit +3): Aunque el buffer no este lleno, el emisor puede forzar a enviarlo.
4. Bit RST (Bit +2): Poniendo este bit, se aborta la conexión. Todos los buffers asociados se vacían.
5. Bit SYN (Bit +1)*:* Este bit sirve para sincronizar los números de secuencia.
6. Bit *FIN (*Bit *+0):* Este bit se utiliza solo cuando se esta cerrando la conexión.

- **Ventana (Window):** Este campo contiene un entero de 32 bits. Se utiliza para indicar el tamaño de buffer disponible que tiene el emisor para recibir datos.
- **Opciones (Options):** Este campo permite que una aplicación negocie durante la configuración de la conexión características como el tamaño máximo del segmento TCP. Si este campo tiene el primer octeto a cero, esto indica que no hay opciones.
- **Relleno (Padding):**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.

- **Checksum:** Mientras que el protocolo IP no tiene ningún mecanismo para garantizar la integridad de los datos, ya que solo comprueba la cabecera del mensaje. El TCP dispone de su propio método para garantizar dicha integridad.

Como en el Checksum del protocolo TCP también se incluyen campos del protocolo IP, es necesario construir una pseudo-cabecera TCP que se considera únicamente a efectos de calculo. (Ver Figura 4.3)

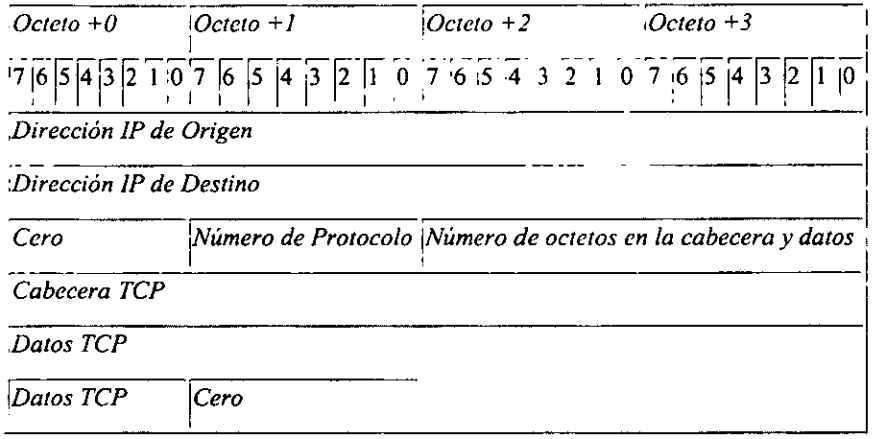

Figura 4. 3 Formato del checksum de TCP

4.6 Estados del TCP

El inicio, mantenimiento y cierre de una conexión requiere que el TCP recuerde toda la información relativa a cada conexión. Esta información se almacena en una entrada para cada conexión dentro del TCB. Cuando se abre una conexión, la entrada en el TCB se realiza con todas las variables inicializadas con sus respectivos valores. Durante la conexión, la entrada del TCB es actualizada a medida que cambia la información. A continuación se describen algunos de los estados del TCP:

- **CLOSED:** No existe, solo para referencia.
- **LISTEN:** Esperando solicitud de conexión de un TCP remoto.
- **SYN-SEN:** Esperando un mensaje de solicitud de conexión después de haber enviado una solicitud de conexión.

- **SYN-RECEIVED:** Esperando confirmación de un reconocimiento de solicitud de conexión, después de haber enviado y recibido una solicitud de conexión.
- **ESTABLISHED:** Representa una conexión abierta. Los datos recibidos pueden ser enviados a un protocolo de una capa superior. Este es el estado normal de la fase de transferencia de la conexión.
- **FIN-WAIT-1:** Esperando la solicitud de fin de conexión de un TCP remoto, o un reconocimiento de una solicitud de fin de transmisión enviada anteriormente.
- **FIN-WAIT-2:** Esperando una solicitud de fin de conexión de un TCP remoto.
- **CLOSE-WAIT:** Esperando una solicitud de fin de conexión de un protocolo de una capa superior.
- **CLOSING:** Esperando el conocimiento de una solicitud de final de conexión de un TCP remoto.
- **LAST-ACK:** Esperando el conocimiento de una solicitud de final de conexión enviada anteriormente al TCP remoto.
- **TIME-WAIT:** Esperando el tiempo necesario para que el TCP remoto haya recibido el conocimiento de la solicitud del fin de conexión.

4.7 Establecimiento de una conexión TCP

Para crear una conexión TCP por la que se empiecen a enviar datos, cada extremo de TCP debe conocer la siguiente información:

- El número de secuencia inicial de los datos que se envían por la tubería de entrada.
- El tamaño de buffer de recepción de datos de la tubería de salida, es decir, el tamaño de la ventana de recepción del otro extremo de la conexión.
- El tamaño máximo de segmento que se puede recibir.
- Las opciones de TCP admitidas.

Número de Puerto	Protocolo de Nivel de aplicación
19	Protocolo de transferencia de noticias en red (NNTP).
20	Servidor de FTP (canal de datos)
21	Servidor de FTP (canal de control)
23	Servidor de Telnet
25	Protocolo simple de transferencia de correo (SMTP)
69	Protocolo trivial de transferencia de archivos (TFTP)
80	Protocolo de transferencia de hipertexto (HTTP) servidor web
139	Servicio de sesión NetBIOS
339	Protocolo de acceso ligero a directorio (LDAP).
445	Bloque de mensajes de servidor (SMB) de hospedaje directo.

Tabla 4. 2 Número de puertos TCP y servicios

Para conocer esta información se intercambian tres segmentos de TCP denominados **proceso de establecimiento de la conexión TCP**, o negociación de tres fases.
Para crear una negociación de TCP, un sistema servidor debe permitir conexiones TCP y un cliente debe iniciar una conexión. El sistema servidor ejecuta una llamada a una función **OPEN pasiva** para permitir solicitudes de conexión entrantes en un número de puerto concreto. La función OPEN pasiva no crea ningún tráfico de TCP. El sistema cliente ejecuta una llamada a la función **OPEN activa** crea y envía el primer segmento de la negociación en tres fases.

Segmento 1 de TCP: Segmento de sincronización, SYN

El extremo A de TCP envía el primer segmento de TCP, conocido como segmento de sincronización, al extremo B (Figura 4.4). El segmento establece los parámetros de la conexión de TCP, como el número inicial de secuencia (ISN) que usará el extremo A

Segmento 2 de TCP: Segmento SYN-ACK

Tras recibir un segmento SYN, el extremo B de TCP envía el segundo segmento conocido como segmento **SYN-ACK,** al extremo A de TCP. El segmento SYN-ACK, establece parámetros de la conexión como el ISN usado por el extremo B y asiente los parámetros de la conexión usados por el extremo A.

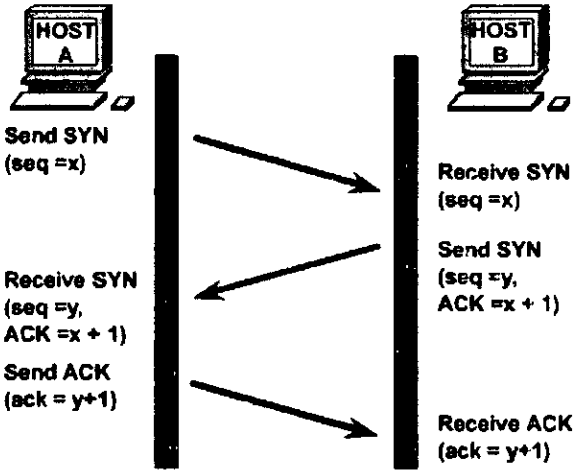

Figura 4.4 Establecimiento de una conexión TCP

Segmento 3: Segmento ACK

Tras recibir el segmento SYN-ACK, el extremo A envía el tercer segmento de TCP, conocido como segmento ACK, al extremo B. El extremo ACK establece los parámetros finales de la conexión de TCP en el extremo A y confirma los parámetros en la conexión de TCP que usa el extremo B.

C A P Í T U L O 5

PROTOCOLOS DE APLICACIÓN

5. CAPA DE APLICACIÓN

Servicio de Nombres de Dominio (DNS)

DNS es un servicio de nombres estándar que permite que un equipo cliente de la red registre y resuelva nombre de dominios. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet. Los tres componentes principales de DNS son los siguientes:

- **Espacio de nombres de dominios y los registros de recursos (RR) asociados.** Una base de datos distribuida de información de nombres.
- **Servidores de nombre de DNS.** Servidores que mantiene el espacio de nombres de dominio y los RR, que responden a las peticiones de los clientes de DNS
- **Resolutores de DNS.** Facilidad con la que un cliente de DNS se pone en contacto con servidores de nombres de DNS y envía peticiones de nombres para obtener información de registro de recursos.

Espacios de nombres de dominio

Es un espacio de nombres jerárquico, estructurado en un árbol que empieza en una raíz sin nombre para todas las operaciones DNS. En el espacio DNS cada nodo y cada hoja del árbol representa un dominio con nombre, donde cada dominio puede tener hijos adicionales.

Nombre de dominio

Un nombre de dominio concreto, es la lista de etiquetas en la ruta desde el nodo nombrada hasta la raiz del árbol DNS.

FTP (File Transfer Protocol).

FTP se usa para compartir y transferir archivos entre equipos, así como para usar otros computadores para el almacenamiento remoto. FTP es un protocolo de nivel de aplicación que utiliza TCP para asegurar la entrega garantizada de datagramas.

SMTP (Simple Mail Transfer Protocol).

SMTP se diseño con el fin de proporcionar mecanismos eficientes y fiables para la transmisión de correo electrónico. SMTP transfiere mensajes de un cliente a un servidor y entre servidores, pero no es responsable del manejo de los buzones de correo ni de permitir al cliente obtener su correo entrante.

TELNET

Permite la conexión a una aplicación remota desde un proceso o terminal.

RPC (Remote Procedure Call).

Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.

SNMP (Simple Network Management Protocol).

Se trata de una aplicación para el control de la red.

NFS (Network File System).

Permite la utilización de archivos distribuidos por los programas de la red.

X-Windows.

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

HTTP

Protocolo utilizado para transferir páginas web, (HTTP Hyper Text Transfer Protocol)

CONCLUSIÓN

CONCLUSIÓN

Con el avance de las comunicaciones y el uso cada vez más creciente de la red de Internet, los protocolos de comunicaciones que componen la suite TCP/IP, han alcanzado una gran importancia en el área de la interconexión de redes de datos, tanto privadas como publicas. Gracias a estos protocolos ha sido posible la Interconexión de equipos de diferentes fabricantes y con diferentes tecnologías.

Al nacer la primera red conectada por medio de este protocolo (*ARPANET*), no se llego a pensar que esta fuera la base para formar una Red Mundial, que proporcionaría un servicio tan importante de información al conectar diferentes sitios, ya no tan sólo entre universidades, si no expandiéndose más haya al conectar negocios, oficinas de gobierno, hospitales, aeropuertos, etc.

Gracias a esta Red conocida como *Internet*, hoy en día se puede acceder a una gran fuente de información a través de las paginas Web, donde se puede consultar desde noticias hasta realizar las compras del hogar; todo esto sin salir de la casa y gracias al desarrollo del protocolo de comunicación TCP/IP.

Con el desarrollo de los protocolos TCP e IP y el nacimiento de la red de *Internet* se han abierto un nuevo campo de exploración en lo que se refiere a redes de carácter mundial, sin embargo el crecimiento de Internet ha venido a plantear una nueva dificultad a estos protocolos. Debido a que cada día se incrementan más sitios a está red mundial, el espacio de direcciones IP existente actualmente, podría verse saturado; para evitar que en un futuro suceda esto, se ha estado desarrollando una nueva versión de este protocolo llamada ***IP versión 6 (IPv6)***, la cual pretende dar solución a este problema.

En este trabajo se dieron los principios de funcionamiento del protocolo TCP e IP, aunque no se trataron los temas a profundidad, se dio una explicación breve de los temas que se consideraron más representativos del funcionamiento de este conjunto de protocolos. Esto con el fin de que este trabajo sirva de base para el estudio formal de los protocolos TCP/IP.

Al tener una base clara del funcionamiento básico de estos protocolos, se puede explorar y entender el funcionamiento de una red IP, en cualquier entorno tecnológico. Es claro que la red formada por Internet seguirá creciendo día a día, por lo que el avance en el desarrollo de una nueva versión de IP (IPv6) es de suma importancia para la evolución de esta red mundial. Además se han desarrollado nuevas aplicaciones como "voz sobre IP", lo cual es un gran avance tecnológico que tendrá una gran relevancia tanto en los hogares como en los negocios, todo esto gracias al desarrollo en los años 70's de los protocolos de comunicaciones TCP/IP.

GLOSARIO DE TERMINOS

Y

ACRÓNIMOS

GLOSARIO DE TERMINOS

ARPANET: Red desarrollada en los años 70's para la interconexión entre universidades de Estados Unidos y Oficinas de Gobierno.

DATAGRAMA: Unidad lógica de información que se envía como unidad de transmisión de datos de una capa de red.

HOST: Sistema de computo, red. Similar al término nodo excepto porque el término Host usualmente se refiere a un equipo de computo.

INTERNET: Se refiere a la interconexión de redes informáticas que permite a las computadoras conectadas comunicarse entre si. El término suele referirse a una interconexión en particular, de carácter público que conecta organismos oficiales, educativos y empresariales.

RFC: (Request For Comment) Serie de documentos que se usan como la principal fuente de información acerca de Internet y sus protocolos. Algunas de estas publicaciones son utilizadas como estándares y otras son de carácter informativo.

PROTOCOLO: Conjunto de normas que regulan la comunicación, establecimiento, mantenimiento y cancelación, entre los dispositivos de una red o de un sistema.

ACRÓNIMOS

ARPA Agencia de Programas Avanzados de Investigación de Estados Unidos

ATM (Asynchronous Transfer Mode). Modo de Transferencia Asíncrono.

BIOS. (Basic Input/Output System). Sistema Básico de Entrada/Salida.

CLI. (Command Line Interface). Interfaz de Línea de Comandos.

CSMA/CD. (Carrier Sense Multiple Access/Collision Detect). Acceso Múltiple con Detección de Portadora y Detección de Colisiones.

DHCP. (Dynamic Host Configuration Protocol). Protocolo de Configuración Dinámica de Servidor.

DLC. (Data Link Control). Control de Enlace de Datos.

DNS. (Domain Name System). Sistema de Nombres de Dominio.

DOS. (Disk Operating System). Sistema Operativo de Disco.

FDDI. (Fiber Distributed-Data Interface). Interfaz de Datos por Distribución de Fibra.

FTP. (File Transfer Protocol). Protocolo de Transferencia de Archivos.

HDLC. (High-Level Data Link Control). Control de Enlace de Datos de Alto Nivel.

HTML. (Hypertext Markup Language). Lenguaje que Señala Hipertexto.

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

ID DE HOST Identificador de Host. Identificador de equipo de computo.

ID DE RED: Identificador de Red.

IEEE. (Institute of Electrical and Electronics Engineers). Instituto de Ingenieros Eléctricos y Electrónicos.

ISO (International Organitation for Standardization) Organización Internacional responsable por una gran cantidad de estándares, incluyendo aquellos referentes a redes. ISO desarrollo el modelo OSI, modelo de referencia para redes.

ICMP (Internet Control Message Protocol) Protocolo que reporta errores y provee información relevante sobre el envió de los paquetes IP.

IP. (Internet Protocol). Protocolo de Internet.

IPX. (Internetwork Packet Exchange). Intercambio de Paquetes entre Redes.

ISDN. (Integrated Services Digital Network). Red Digital de Servicios Integrados.

LAN. (Local Area Network). Red de Área Local

MAN. (Metropolitan Area Network). Red de Área Metropolitana.

MP3. (MPEG-1 Audio Layer-3).

MTU: (Maximum Transmission Unit) Cantidad máxima de paquetes, en bytes, que puede manejar una interfaz en particular.

NDIS. (Network Driver Interface Specification). Especificación de Interfaz para el Controlador de Red.

NDS. (Novell Directory Services). Servicio de Directorios de Novell.

NetBEUI. (NetBIOS Extended User Interface). Interfaz Extendida de Usuario NetBIOS.

NetBIOS. (Network Basic Input/Output System). Sistema de Red Básico de Entrada/Salida.

NFS. (Network File System). Sistema de Archivos de Red.

NIC. (Network Interface Card). Tarjeta de Interfaz de Red.

NOS. (Network Operating System). Sistema Operativo de Red.

NTFS. (NT File System). Sistema de Archivos de NT.

ODI. (Open Data-Link Interface). Interfaz de Enlace de Datos Abierta.

PC. (Personal Computer). Computadora Personal.

PMTU: (Path Maximum Transmission Unit) Descubrimiento de la unidad máxima de transmisión.

POP3. (Post Office Protocol 3). Protocolo de Servicio Postal 3.

POSIX. (Portable Operating System Interface). Interfaz de Sistema Operativo Portable.

PPP. (Point-to-Point Protocol). Protocolo Punto a Punto.

PPTP. (Point-to-Point Tunneling Protocol). Protocolo Punto a Punto por Tuneleo.

SCSI. (Small Computer System Interface). Interfaz de Sistema de Computadoras Pequeñas.

SMB. (Server Message Block). Bloque de Mensajes del Servidor.

SMTP. (Simple Mail Transfer Protocol). Protocolo de Transferencia de Correo Simple.

SNA. (Systems Network Architecture). Arquitectura de Sistemas de Red.

SOHO. (Small Office Home Office). Oficina en Casa/Oficina Pequeña.

TCB Bloque de Control de Transmisión.

TCP/IP. (Transmission Control Protocol/Internet Protocol). Protocolo de Control de Transmisión/Protocolo de Internet.

TOS (Type of Service) Campo de la cabecera IP que define la calidad de transmisión de un datagrama IP.

TTL (Time To Live) Campo de la cabecera IP, que indica cuanto tiempo puede durar un paquete IP en la red sin considerarse no valido.

NAT: (Network Address Translator) Dispositivo que se encarga de convertir una dirección IP privada en pública.

UDP: (User Datagram Protocol) Protocolo perteneciente a la capa de transporte del modelo TCP/IP. Este protocolo se encarga del intercambio de datagramas sin confirmar si llegaron bien al destino.

URL. (Uniform Resource Locator). Localizador Uniforme de Recursos.

UUCP. (UNIX-to-UNIX Copy Protocol). Protocolo de Copia UNIX a UNIX.

WAN. (Wide Area Network). Red de Área Amplia.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Thomas Lee
Joseph Davis
Windows 2000 TCP/IP
Protocolos y servicios
Mc Graw Hill

http://www4.uji.es/~al019803/Tcpip.htm

Ing. Gustavo Cárdenas Cerros
Introducción a las Redes de
Datos V
Alcatel

Microsoft Training and Certification
Internetworking with Microsoft
TCP/IP on Microsoft Windows
NT 4.0

Thomas W. Madron
Redes de área local
Ed. Limusa,1993

Uyless Black
Redes de computadoras, protocolos, normas e interfaces
2ª ed., Ed. Computec-rama

Gilbert Held

Understanding data communications

Ed. Wiley & Sons,1991, England

Andrew Tanenbaum

Redes de ordenadores

2ª ed.. Ed. Prentice Hall,1991, México

RFC 793 TCP Transmission Control Protocol

RFC 768 User Datagram Protocol

RFC 791 The Internet Protocol

RFC 792 Internet Control Message Protocol