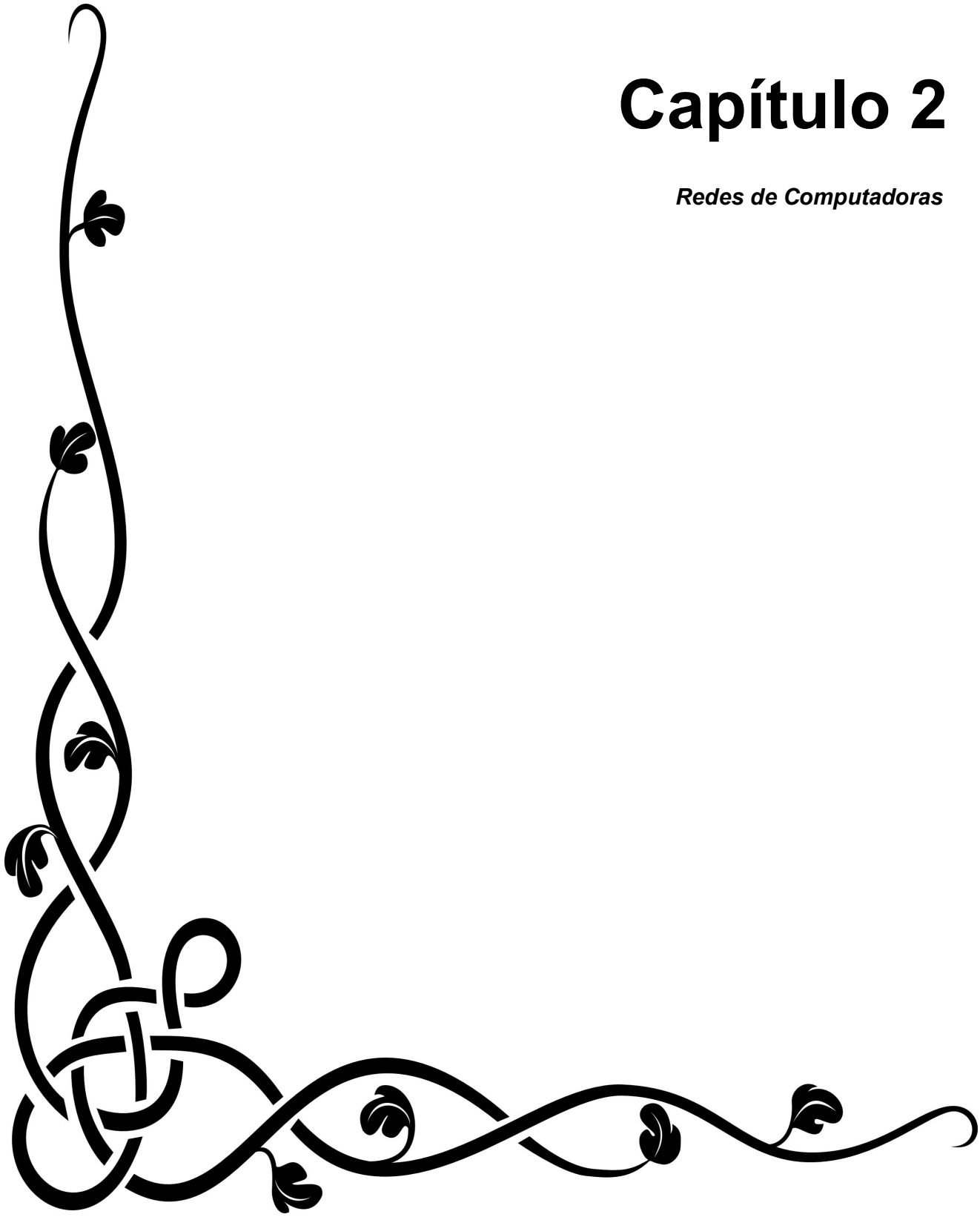
Capítulo 2

Redes de Computadoras



"¿Por qué esta magnífica tecnología científica, que ahorra trabajo y nos hace la vida más fácil, nos aporta tan poca felicidad? La repuesta es esta, simplemente porque aún no hemos aprendido a usarla con tino."
Albert Einstein

Redes de Computadoras

2.1 Conceptos Básicos

El concepto de redes no solo es aplicable al contexto de las computadoras, un conjunto de células o un conjunto de personas también son consideradas una red, pero sin importar la forma en que estén implementadas, tienen el mismo objetivo: la comunicación. Para lograr ésta comunicación es necesario un medio para transmitir la información, y un sistema que nos indique cómo transmitir esa información.

En este capítulo me enfocaré en los términos básicos para entender cómo se conforma una red de computadoras.

2.1.1 Red de Computadoras

Es un conjunto de dos o más computadoras independientes que se encuentran interconectadas entre sí con el propósito de intercambiar información y compartir recursos. Pueden configurarse usando diferentes topologías físicas. El medio para establecer la conexión varía de acuerdo a las necesidades del usuario, puede usarse cable de cobre, fibra óptica y aire (microondas, luz infrarroja y satélites de comunicación).

2.1.2 Clasificación de Redes

Para facilitar el estudio de las redes de computadoras, se han realizado diversas clasificaciones, dos de las más aceptadas son las siguientes:

1. Por tecnología de transmisión.
2. Por su extensión geográfica.

2.1.2.1 Clasificación por tecnología de transmisión

Las tecnologías más utilizadas actualmente son:

Redes de Difusión

Este tipo de redes tienen un solo canal de transmisión que comparten todos los equipos (nodos). El envío de un mensaje (paquete) es recibido por todos los nodos, cada paquete cuenta con un campo de dirección que específica a quien va dirigido. La máquina que recibe el paquete verifica el campo de dirección y comprueba si esta dirigido a ella, si es así lo procesa, en caso contrario lo ignora.

Al colocar un código especial en el campo de dirección el sistema de difusión permite que todos los nodos procesen el paquete recibido, a este método se le conoce como difusión (broadcasting). Si la transmisión se realiza a un subconjunto de nodos se le llama multidifusión (multicasting).

Redes de Punto a Punto

Las redes punto a punto constan de muchas conexiones de pares de nodos. En este tipo de redes es importante encontrar la ruta correcta. Por eso al realizar una transferencia, es probable que el paquete tenga que visitar uno o más nodos. La transmisión de punto a punto entre emisor y receptor se conoce como unidifusión (unicasting).

En general se recomienda usar difusión cuando se implementa una red dentro de una misma área geográfica, o punto a punto cuando es una red más grande.

2.1.2.2 Clasificación por su extensión geográfica

Otra forma de clasificar las redes es considerando la extensión física que ocupan sus componentes, se dividen en 5 categorías.

Redes de Área Personal (PANs)

Son las redes destinadas para uso personal, la comunicación se realiza entre distintos dispositivos (computadoras con mouse y teclado inalámbrico, impresoras, PDAs, teléfonos celulares apoyados en funciones como Bluetooth, dispositivos de audio, cámaras fotográficas, etc.) que se encuentran cerca.

Redes de Área Local (LANs)

Son las redes de propiedad privada, su extensión comprende desde un edificio hasta un campus. Su mayor aplicación es la interconexión de PC's con estaciones de trabajo en oficinas, fábricas y universidades para compartir recursos (impresoras, faxes) e intercambiar datos y aplicaciones (bases de datos, software, ancho de banda). Hay tres aspectos importantes que distinguen a las LANs de otro tipo de redes:

Extensión física.

Tecnología de transmisión.

Topología.

Redes de Área Metropolitana (MANs)

Redes de comunicación de alta velocidad, permiten la interconexión de varias LANs cercanas geográficamente ofreciendo cobertura en un área más extensa, también proporcionan la integración de múltiples servicios mediante la transmisión de datos, voz y video. El ejemplo más común de una MAN es la televisión por cable.

Redes de Área Amplia (WANs)

Redes diseñadas para satisfacer áreas geográficas tan extensas como países y continentes. Compuesta por un conjunto de máquinas dedicadas a ejecutar aplicaciones de usuarios. A cada usuario se le llama host y estos están conectados por una subred (compañía telefónica o proveedor del servicio de Internet) la cual tiene la función principal de conducir mensajes de un *host* a otro.

Internet

Internet es un conjunto global de diferentes redes de comunicación que utilizan la familia de protocolos TCP/IP. Se encarga de interconectar computadoras y estaciones de trabajo en todo el mundo con la finalidad de intercambiar datos e información.

En la Tabla 2.1 podemos observar la extensión que se recomienda para cada tipo de red.

Distancia entre computadoras	Ubicación	Ejemplo
1 m	Metro cuadrado	Red de Área Personal
10 m	Cuarto	Red de Área Local
100 m	Edificio	
1 Km	Campus	
10 Km	Ciudad	Red de Área Metropolitana
100 Km	País	Red de Área Amplia
1,000 Km	Continente	
10,000 Km	Planeta	Internet

Tabla 2.1 *Clasificación de computadoras interconectadas por escala*[2]

2.1.3 Topologías de Red

Cuando hablamos de topología nos referimos a la disposición física de los dispositivos o nodos de una red, para lograr la interconexión entre ellos a través de un medio de comunicación.

Existen cuatro topologías básicas:

1. Topología de Bus
2. Topología de Anillo
3. Topología de Estrella
4. Topología de Malla

A continuación se explica brevemente en qué consiste cada una de estas configuraciones.

[2] Fuente: Andrews S. Tanenbaum “Redes de Computadoras”

Topología de Bus

Se caracteriza porque todos sus nodos comparten el mismo canal de comunicación a través de un medio multipunto (Figura 2.1). La información que se transmite se propaga por todo el bus y llega a todos los nodos, cada nodo es capaz de reconocer cuando la información está destinada a él. Tiene un ancho de banda de 10 Mbps.

Ventajas

- Es de fácil implementación y crecimiento.
- Económica

Desventajas

- La longitud máxima del bus se encuentra entre 185 y 200 m.
- Si hay problemas con el cable o llega a romperse, toda la red dejará de funcionar.
- Se requieren terminadores en cada extremo del bus.
- Hay colisiones cuando varios nodos quieren transmitir al mismo tiempo, ya que solo hay un canal de transmisión.

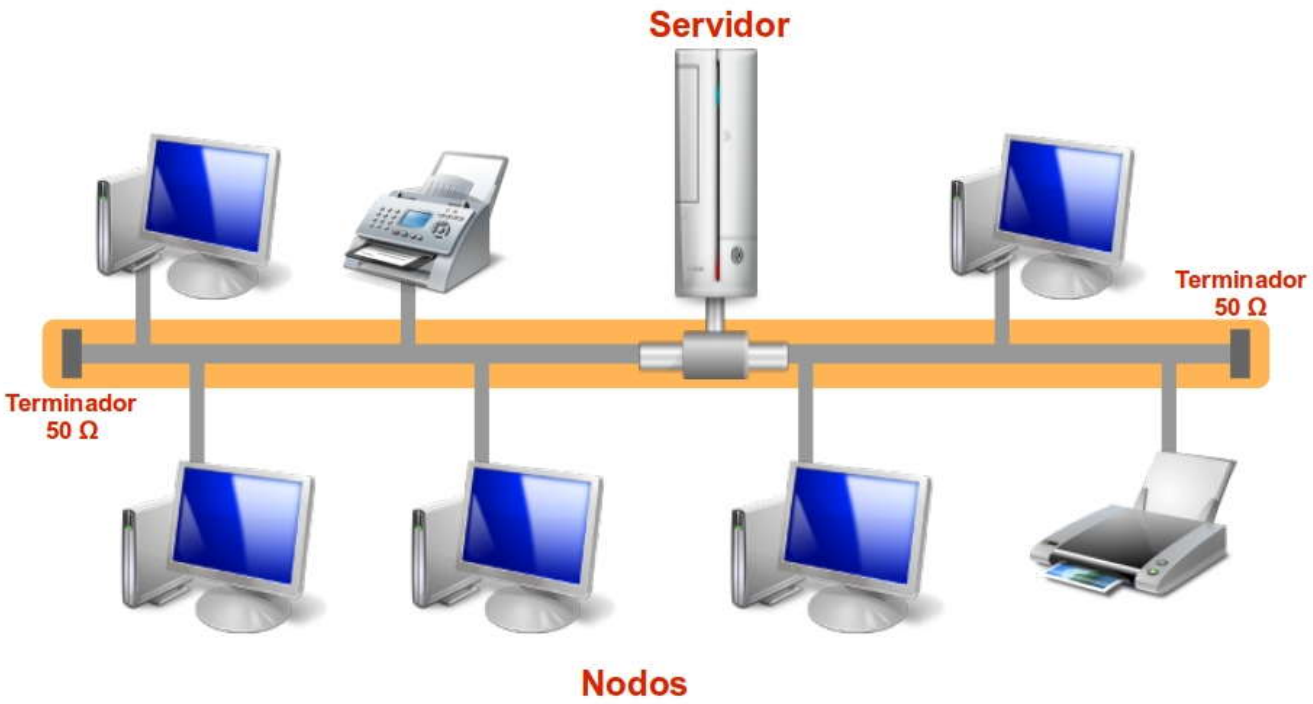


Figura 2.1 *Topología de Bus*

Topología de Anillo

Los nodos de la red están interconectados entre si mediante un anillo cerrado (Figura 2.2). Cada nodo consta de un receptor y un transmisor que hacen la función de repetidor. El conjunto de repetidores están unidos mediante enlaces punto a punto.

La información se transmite en un solo sentido, el acceso al medio de la red se realiza por medio de un *token* o testigo. Si un nodo quiere enviar información crea un *token* y lo envía a través del anillo pasando por todos los nodos hasta llegar al nodo destino, quien enviará un mensaje al nodo origen para indicar que recibió la información. Tiene un ancho de banda de 4 a 16 Mbps.

Ventajas

- Es fácil aumentar o disminuir la cantidad de nodos.
- Se puede implementar un anillo doble para transmitir información en dos sentidos.

Desventajas

- Es difícil localizar los problemas en el canal de comunicación lo que puede paralizar o bloquear a toda la red.
- Entre mayor sea el flujo de información, la velocidad de respuesta de la red será menor.

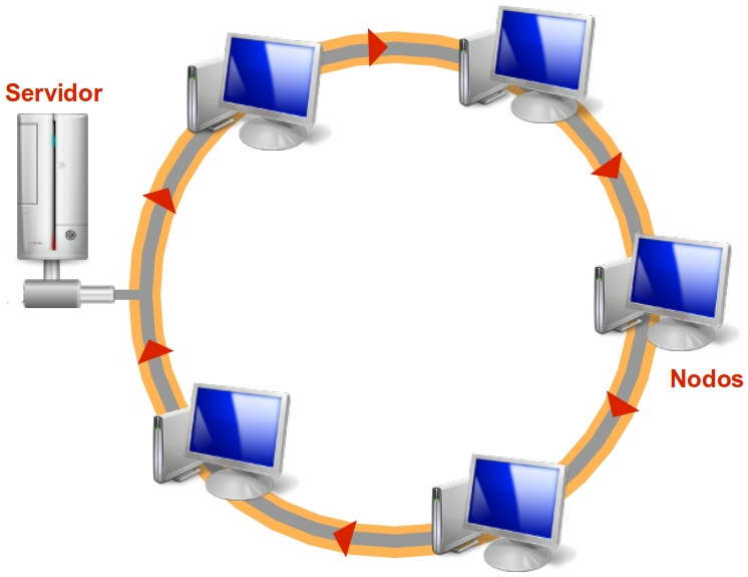


***Figura 2.2** Topología de Anillo*

Topología de Estrella

En esta red los nodos están directamente conectados a un nodo central (*hub*, *switch* o *router*) común mediante un enlace punto a punto dedicado y un puerto de entrada/salida para transmisión y recepción. Se puede observar una representación en la Figura 2.3.

Si un nodo quiere enviar información a otro equipo, primero debe enviarla al nodo central y éste se encargará de enviara al nodo destino. En la actualidad el ancho de banda puede ser hasta de 10Gbps.

Ventajas

- Es fácil agregar nodos y reconfigurar la red.
- Si un nodo se desconecta o tiene un fallo, no afecta en el funcionamiento de toda la red.

Desventajas

- La red se desconectará si el nodo central deja de funcionar.
- Es más costosa debido al equipo empleado como nodo central y al uso de mayor cantidad de cable.

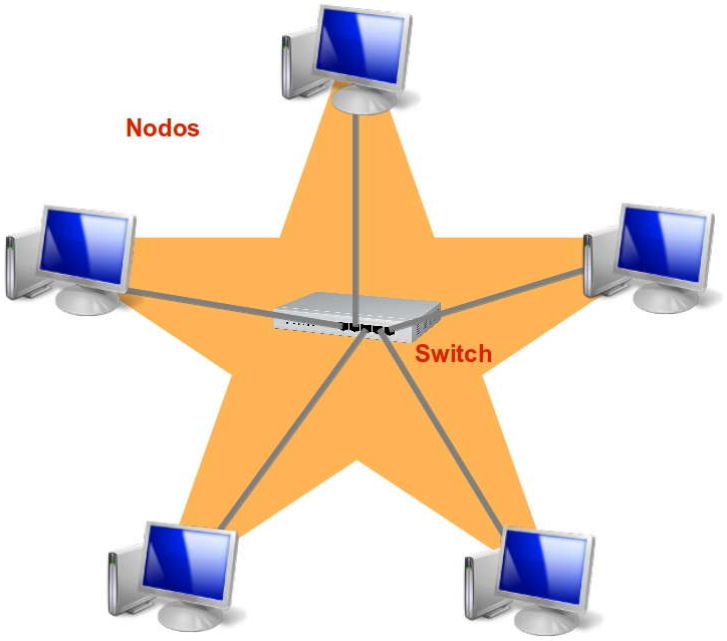


Figura 2.3 *Topología de Estrella*

Topología de Malla

En este tipo de topología cada nodo de la red está conectado a todos los demás nodos mediante enlaces punto a punto. Esta configuración facilita el envío de información ya que se puede enviar por diferentes rutas. En la Figura 2.4 se ilustra un ejemplo.

Ventajas

- Es tolerante a fallas gracias a la redundancia de sus conexiones.
- Si un cable se rompe no inhabilita a toda la red.
- Se pueden agregar nuevos nodos sin afectar a los que ya existen.

Desventajas

- Su implementación y configuración son complicadas debido a la gran cantidad de conexiones.
- Es muy cara ya que requiere más cable que cualquier otra topología.

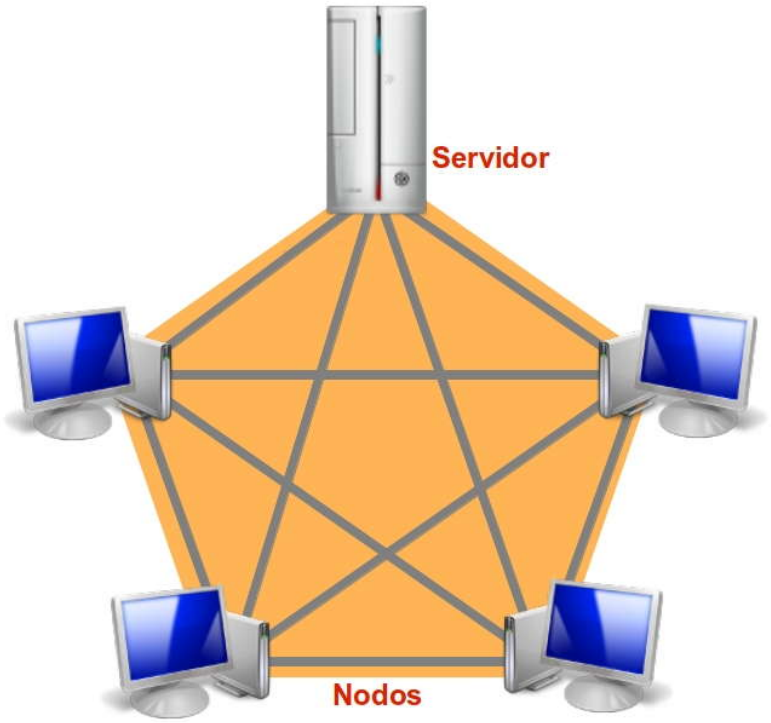


Figura 2.4 *Topología de Malla*

2.1.4 Modelos de Referencia

Debido al crecimiento acelerado de las telecomunicaciones y la informática los fabricantes de equipos comenzaron a tener problemas, ya que lograr una comunicación con equipos de diferentes fabricantes era muy complicado o casi imposible debido a la cantidad de especificaciones e implementaciones en la tecnología de red. La necesidad de crear estándares para lograr una interconexión entre redes informáticas se hizo evidente y en 1977 la ISO (Organización Internacional para la Estandarización) realizó una investigación para tener un conjunto de reglas aplicables en todas las redes, así creo el modelo OSI (Interconexión de Sistemas Abiertos) el cual fue adoptado como estándar internacional hasta 1984.

Por otro lado, el modelo TCP/IP fue desarrollado por los científicos Vinton Cerf y Robert Khan en 1974 durante su participación en el proyecto ARPANET para lograr conectar múltiples redes independientemente del hardware con el que se implementaran, crearon una arquitectura de protocolos de comunicación que facilitaba el intercambio de información y que aún en la actualidad sigue siendo la más utilizada.

2.1.4.1 Modelo OSI (Interconexión de Sistemas Abiertos)

El modelo OSI, ilustrado en la Figura 2.5, está basado en la idea de que el proceso de comunicación entre dos nodos puede dividirse en 7 capas:

La capa física

En esta capa se encuentran todos los medios físicos que intervienen en la comunicación, además se encarga de controlar los puertos ó circuitos de los dispositivos utilizados para garantizar la transmisión de información. Las características más importantes a considerar son las propiedades físicas y especificaciones de los conectores, cómo representar un bit y cómo interactúa el medio físico con el medio de transmisión.

La capa de enlace de datos

El trabajo principal de esta capa es hacer que el enlace físico sea fiable, y que la información que se transmite llegue sin errores a su destino, además determina cuando y quien puede acceder al medio.

Los datos son segmentados en tramas y se emplea el *direccionamiento físico*[3] para garantizar que llegarán a su destino. Esta capa se caracteriza por tener un control de flujo y un manejo de errores.

La capa de red

El objetivo de ésta capa es hacer que los datos lleguen de un origen a un destino a través de una red de comunicación. Tanto el emisor como el receptor pueden estar configurados de forma diferente (pueden usar distintos protocolos), por lo que ésta capa resuelve los problemas de compatibilidad. Por medio del *direccionamiento lógico*[4] se determina la ruta de los datos y su receptor final.

Cuenta con un control de la congestión de red, elemento necesario para saber cuando la saturación de un nodo puede llegar a bloquear la red.

La capa de transporte

Esta capa es el corazón de la comunicación, ya que aísla a las capas superiores de los cambios en la tecnología del hardware y además garantiza la entrega de los datos sin errores, en orden y sin pérdidas.

Recibe los datos de las capas superiores y los segmenta para transmitirlos a la capa de red y los reensambla en el nodo destino. En esta capa se determina el tipo de servicio que se proporciona a la capa de sesión para ofrecer un servicio de calidad al usuario final.

La capa de sesión

Esta capa permite que se establezcan sesiones entre diferentes máquinas. Inicia, mantiene y termina la comunicación. Los principales servicios que ofrece es la de control de diálogo, la *sincronización*[5] y la administración de concurrencia.

[3] Dirección física que seguirán las tramas, es única ya que identifica al fabricante y al hardware de red.
[4] Dirección IP que identifica a un equipo de cómputo en una red interna o externa.
[5] Establecer puntos de referencia para recuperar una transferencia en caso de que sea interrumpida.

La capa de presentación

Esta capa se encarga de la forma en la que se presenta la información. Está relacionada con el significado, la interpretación y la coordinación de los datos. Tiene la función de que la información enviada por el nodo inicial sea recibida por el nodo final.

La capa de aplicación

Es la capa más cercana al usuario y ofrece la posibilidad de acceder a los servicios de las otras capas. Se define la interfaz para la comunicación entre el software y la red. Los usuarios no tienen trato directo con ésta capa, son los programas los que interactúan con ella. Algunos ejemplos de aplicaciones de uso común son la transferencia de archivos, el correo electrónico y el acceso a computadoras por medio de terminales.

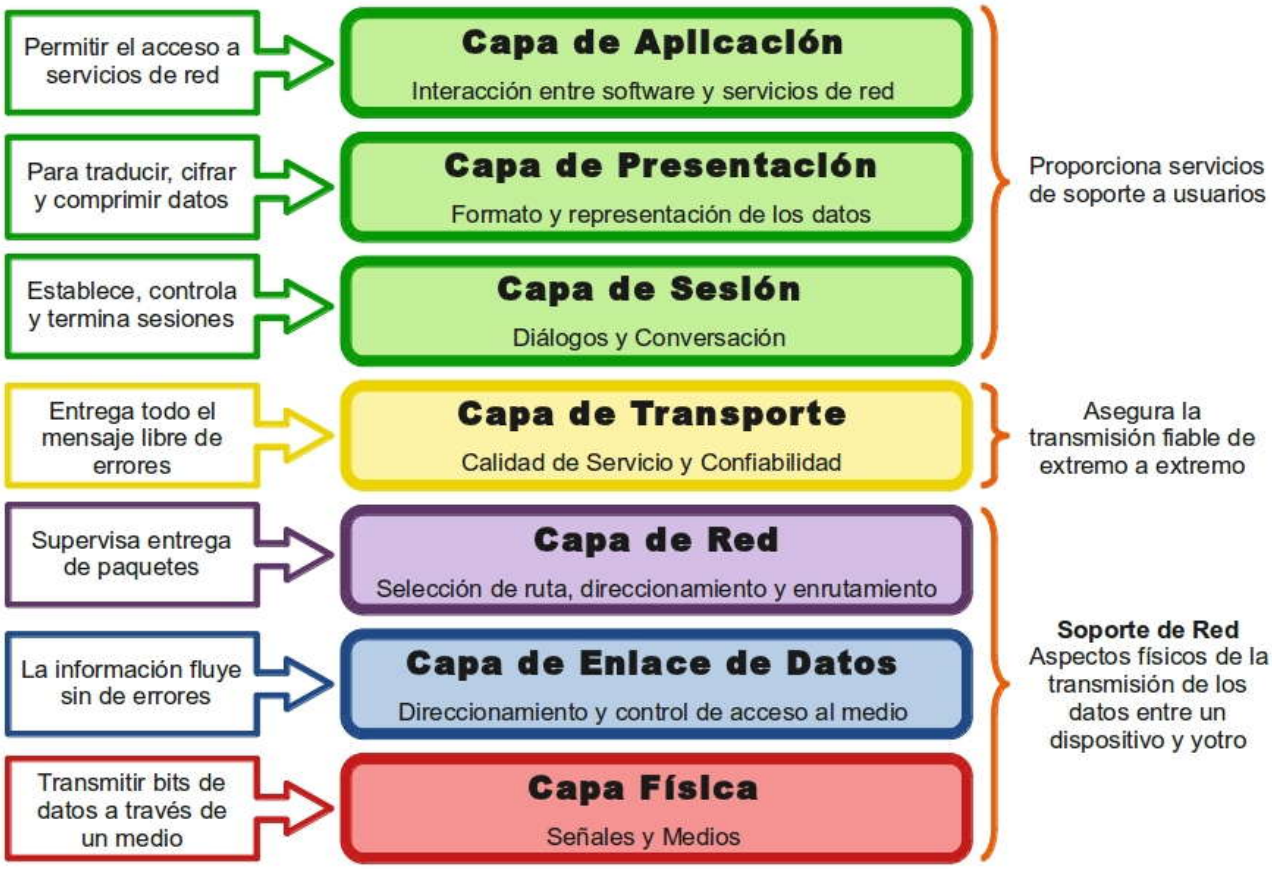


Figura 2.5 *Las capas del modelo de referencia OSI*

2.1.4.2 Modelo TCP/IP

Llamado así por los dos protocolos más importantes que lo componen, el TCP (Protocolo de Control de Transmisión) y el IP (Protocolo de Internet), pero en realidad está compuesto por un grupo extenso de protocolos. Podemos observar una representación del modelo en la Figura 2.6. Está dividido en 4 capas:

La capa de host a red

En este nivel el *host* establece una conexión con los medios físicos de la red mediante el protocolo TCP/IP para enviar paquetes IP. Éste protocolo puede variar de *host* a *host* ya que no está definido.

La capa de interred

La capa de interred es la que mantiene unida a toda la arquitectura y se considera similar en funcionalidad a la capa de red del modelo OSI. En ésta capa se permite el traslado independiente y se gestiona la entrega de los paquetes IP a su destino. El protocolo principal que se define y trabaja en ésta capa es el IP. Un aspecto muy importante a considerar es el enrutamiento, ya que tiene como propósito evitar la congestión en la red.

La capa de transporte

Esta capa permite que un *host* origen establezca una conversación con el *host* destino (similar al comportamiento de la capa de transporte en el modelo OSI). Se definen dos protocolos de transporte importante, el primero de ellos es el TCP, el cual es confiable y está orientado a la conexión por lo que el mensaje debe entregarse sin errores, el flujo de bytes se segmenta en pequeños mensajes y los pasa a la capa de interred, en el *host* destino el protocolo TCP se encarga de reensamblar los mensajes. El TCP también cuenta con un control de flujo.

El segundo protocolo es el UDP (Protocolo de Datagrama de Usuario), no es confiable y no está orientado a la conexión. Tiene un amplio uso de consultas únicas de tipo cliente-servidor y aplicaciones de entrega puntual tales como voz y video.

La capa de aplicación

En esta capa se realiza la comunicación entre programas de red usando protocolos de alto nivel, además de manejar los aspectos de representación, codificación y control del diálogo. Algunos ejemplo de las aplicaciones más utilizadas por los usuarios con sus respectivos protocolos son:

- La terminal remota (SSH - Interprete de Comandos Seguro).
- Transferencia de archivos (FTP - Protocolo de Transferencia de Archivos).
- El correo electrónico (SMTP - Protocolo Simple de Transferencia de Correo).
- La administración de red (SNMP – Protocolo Simple de Administración de Red).
- Y la resolución de nombres (DNS – Sistema de Nombres de Dominio).

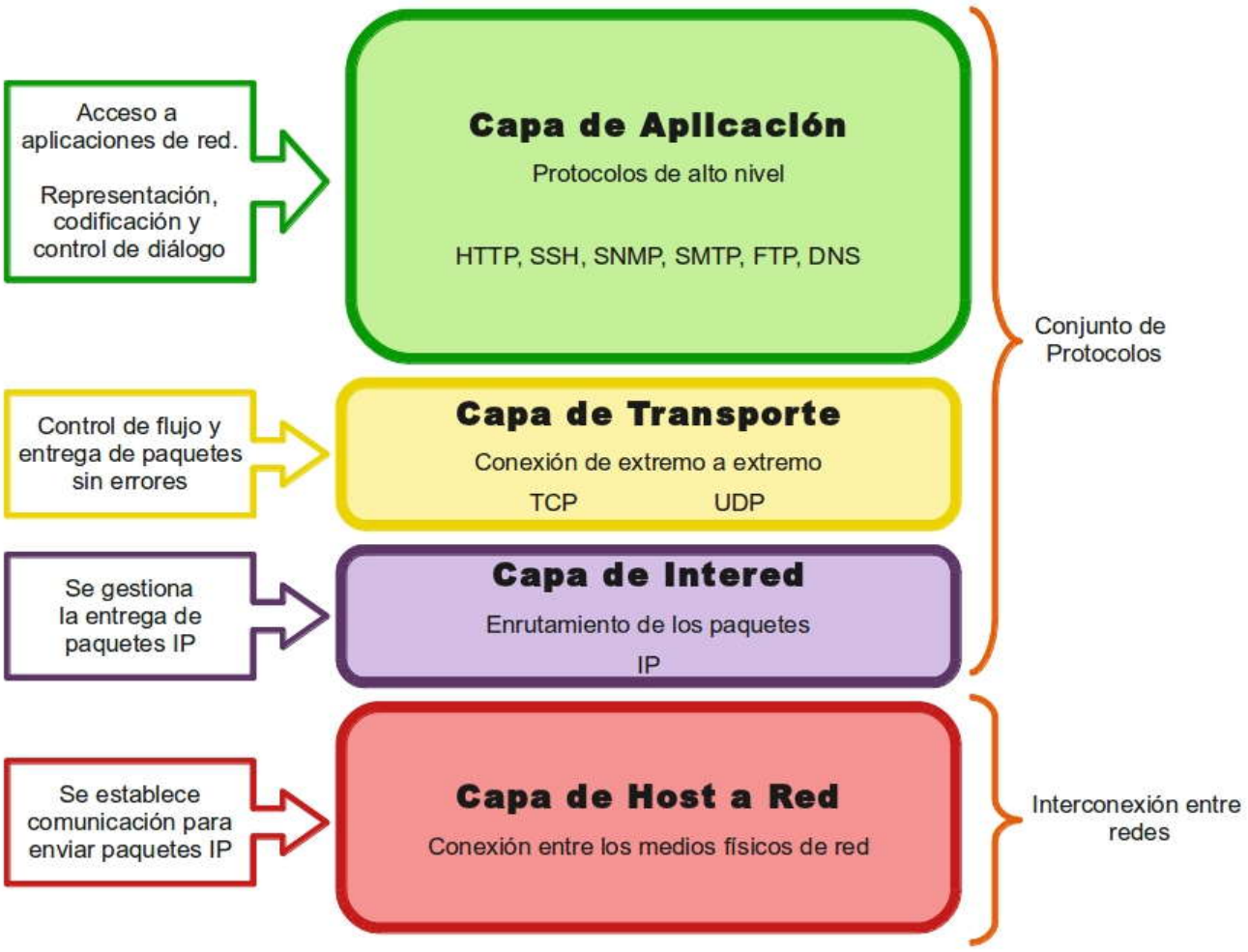


Figura 2.6 *Las capas del modelo de referencia TCP/IP*

2.2 Control de Acceso al Medio (MAC – Media Access Control)

El administrador de la red de datos del Instituto de Física solicitó un registro de las direcciones MAC's de los usuarios de la red, por lo que es importante explicar en qué consisten dichas direcciones físicas. A continuación se da una breve descripción.

La dirección MAC es un identificador único compuesto de 12 dígitos hexadecimales (48 bits de longitud), éste es asignado y escrito de forma binaria directamente en los dispositivos de red durante su fabricación con el objetivo de lograr el reconocimiento de cada dispositivo a nivel mundial.

Por convención, el formato de escritura que sigue la dirección MAC puede ser de las siguientes dos formas:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS

Los primeros 6 dígitos (24 bits) sirven para identificar al fabricante del dispositivo, éstos son asignados por la ***OUI (Organizationally Unique Identifere - Identificador Único Organizacional)***, quien a su vez compra bloques, con sus posibles derivados de direcciones, administrados por la ***IEEE (Institute of Electrical and Electronics Engineers – Instituto de Ingeniería Eléctrica y Electrónica)*** para identificar mundialmente a cada empresa u organización y poder asegurar la singularidad de cada dispositivo. Los últimos 6 dígitos (24 bits) son asignados por el fabricante de forma secuencial durante su fabricación en el momento del Quemado de las Direcciones ***(BIA – Burned-In Address)***.

Cada tarjeta de red cuenta con un conjunto de chips encargados de administrar la comunicación con los *medios físicos* [6] controlando las *señales de comunicación* [7] de dichos medios.

[6] Cable, fibra óptica, aire, etc.
[7] Electricidad, luz o frecuencia de radio

La MAC se encarga de proporcionar los medios para acceder al medio físico usado en la comunicación. Su principal objetivo es hacer que la información fluya libre de errores entre dos máquinas conectadas.

2.3 Dirección IP

Una dirección IP es un identificador numérico único que permite referirse lógicamente a una interfaz de red.

Cada host y enrutador de Internet tiene una dirección IP, que codifica su número de red y su número de host. La combinación es única: no hay dos máquinas que tengan la misma dirección IP.[8]

El objetivo de estas direcciones es permitir la comunicación entre hosts, ya que al ser irrepetibles es fácil identificar a cada uno de ellos dentro de una red.

En la actualidad existen 2 tipos de direcciones, a continuación se realiza una breve descripción de ellas.

Direcciones IPv4

Las direcciones IPv4 se expresan con una notación decimal y tienen una longitud de 32 bits (2^{32} direcciones), se representan por 4 octetos separados por un "**.**" y pueden estar comprendidos entre 0 a 255.

Ejemplo de IPv4: 132.248.7.15

Direcciones IPv6

Debido al incremento del uso de Internet en el mundo, la gran demanda de direcciones IP provocó que las direcciones IPv4 fueran insuficientes, por lo que se creó una nueva generación para otorgar una cantidad significativa de direcciones.

[8] Fuente: Andrews S. Tanenbaum "Redes de Computadoras"

Las direcciones IPv6 tiene una expresión hexadecimal, con una longuitud de 128 bits (2^{128} direcciones) representados por 8 grupos de 16 bits y separados por "**:**", pueden estar comprendidos entre 0000 a FFFF

Ejemplo de IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Estas direcciones no son sensibles a mayúsculas/minúsculas. Están conformadas por 2 partes lógicas, la primera parte es un prefijo con los 64 bits más significativos, la segunda parte con los 64 bits menos significativos se genera automáticamente a partir de las direcciones mac.

2.4 El Modelo Cliente/Servidor

El modelo Cliente/Servidor es una arquitectura distribuida donde las transacciones se dividen en procesos independientes que cooperan entre si para intercambiar servicios, recursos o información. El cliente inicia el diálogo solicitando un servicio y el servidor envía uno o más mensajes respondiendo a la petición.

El servidor presenta a los clientes una interfaz bien definida, los clientes solo conocen la interfaz externa del servidor y no dependen de su ubicación física, del equipo físico que lo conforma ni del sistema operativo con el que trabaja.

Servidor

Un servidor es una máquina encargada de proporcionar servicios dentro de una red, con el propósito de compartir sus recursos con usuarios a los que se les conoce como clientes. Hay diversos tipos de servidores que satisfacen las necesidades de los usuarios, algunos ejemplos más conocidos son los servidores de correo, los servidores web, los servidores de archivos, los servidores de aplicaciones y los servidores de impresión.

Cliente

Un cliente es una máquina o una aplicación que se utiliza para acceder a los servicios que

ofrece un servidor. Es el proceso que permite al usuario formular una solicitud al servidor para consultar datos externos, interactuar con otros usuarios, compartir su información o para utilizar recursos de los que no dispone en su máquina local.

2.5 Protocolo SSH (Protocolo de conexiones seguras)

El protocolo SSH fue creado por el investigador finlandés Tatu Ylönen en 1995 después de que su red sufrió un ataque de *sniffing*[9]. Su implementación fue liberada como *freeware*[10] y tuvo tanto éxito que llegó a reemplazar a los protocolos *telnet*, *rlogin* y *rsh*, ya que no garantizaban seguridad y confidencialidad. Este protocolo opera en la capa de aplicación, facilita una comunicación segura entre dos sistemas usando una arquitectura cliente/servidor y realizando la conexión de forma remota, es decir, no es necesario estar físicamente frente al equipo, se controla a través de una interfaz de línea de comandos. El intercambio de datos se realiza usando un canal seguro entre dos dispositivos de red. SSH cifra toda la información (incluyendo las contraseñas) para evitar que terceros la intercepten ya que solo verán un conjunto de símbolos ininteligibles.

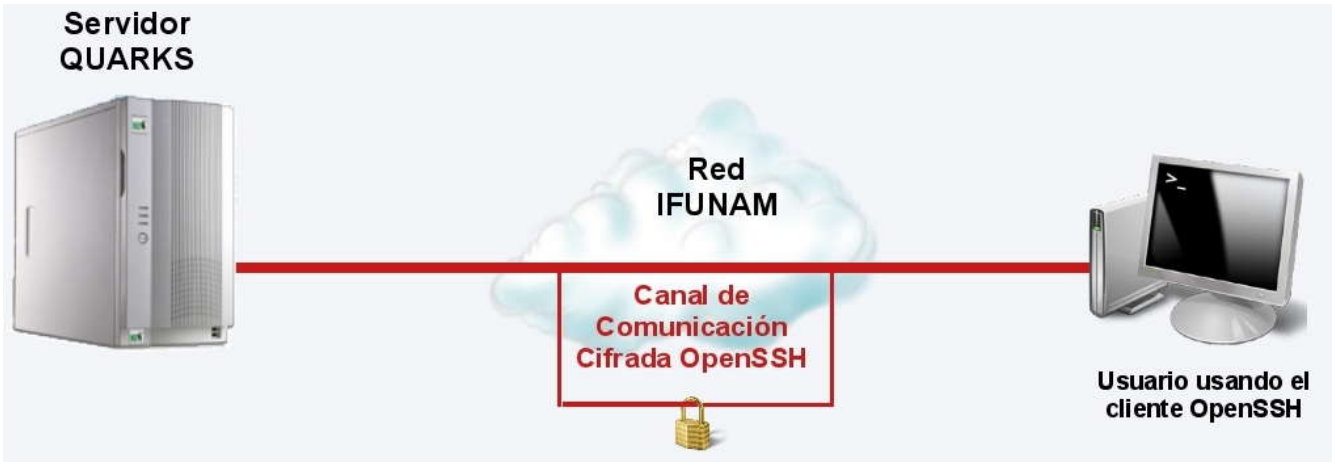


Figura 2.7 *Ejemplo de conexión usando el protocolo SSH*

Tuvo mucho éxito gracias a que sus principales aplicaciones son el logueo, la autenticación

[9] Interceptar la información que circula por una red informática.
[10] Distribución libre o gratuita de programas.

de usuarios, la transferencia de archivos, la ejecución de comandos y consideradas como las más importantes, la codificación del mensaje, la autenticación de equipos y la integridad del mensaje.

En nuestro caso usaremos la distribución libre OpenSSH, la cual es desarrollada por el proyecto OpenBSD, cuyo código puede usarse libremente bajo la licencia BSD.

Los programas integrados a OpenSSH son:

- ssh: programa cliente que sirve para loguearse a una máquina remota y nos permite ejecutar comandos.
- scp: nos permite realizar copias seguras de documentos entre *hosts*.
- sftp: programa de transferencia segura de archivos, muy similar a ftp, el cual realiza las operaciones de transporte de datos sobre un canal cifrado.
- sshd: es el demonio del programa ssh y se ejecuta constantemente en el servidor, esperando que soliciten una conexión.
- ssh-keygen: se encarga de generar, controlar y convertir las llaves autentificadas.

2.6 Protocolos de Comunicación

La configuración, el funcionamiento y el contenido de las capas puede variar de red en red por lo que para lograr una comunicación entre equipos, que pueden ser de fabricantes diferentes y usar diversos sistemas operativos, se crearon los protocolos de comunicación, que pueden definirse como el conjunto de reglas y estándares que especifican como debe realizarse la comunicación y el intercambio de datos entre dos sistemas.

2.6.1 Protocolo TCP (Protocolo de Control de Transmisión)

El protocolo de comunicación TCP fue desarrollado basándose en los conceptos descritos en 1974 por los científicos Vinton Cerf y Robert Khan, se diseñó para permitir una conexión de extremo a extremo entre redes fiables y no fiables y proveer las funciones necesarias para una aplicación de transporte de flujo de bytes sin errores.

El protocolo TCP fragmenta la información en paquetes, llamados segmento TCP, a los que les añade un encabezado con formato fijo de 20 bytes seguido de 0 o más bytes de datos. Este protocolo decide el tamaño de los segmentos, cuándo enviar los datos y cuándo bloquear la información.

Para lograr que la comunicación entre los *hosts* sea confiable el protocolo realiza operaciones específicas con mecanismos de diversas áreas, estos mecanismos y sus funciones principales en cada una de ellas son:

Transferencia básica de datos: TCP es capaz de transferir un flujo continuo de octetos empaquetados en segmentos para su transmisión a través de una red. Si el usuario especifica un bloque de datos como urgente TCP marcara el final de dicho bloque como un puntero de urgente y lo enviará en el flujo de datos ordinario.

Fiabilidad: TCP debe recuperar la información corrupta, perdida, duplicada o desordenada, para lograrlo asigna una secuencia a cada octeto que transmite y exige un acuse de recibo (ACK) del receptor, si no lo recibe en cierto tiempo los datos se retransmiten. El receptor usa los números de secuencia para ordenar los segmentos y así evitar la duplicidad. Para descartar los segmentos dañados se añade una suma de control (cheksum) a cada segmento transmitido que se comprueba en el receptor. TCP es capaz de recuperarse cuando hay errores en la comunicación.

Flujo de control: Con ayuda de TCP el receptor puede controlar la cantidad de datos enviados por el emisor, en cada ACK envía una “ventana” que indica la cantidad de octetos que el emisor tiene permitido transmitir antes de recibir el próximo permiso.

Multiplexamiento: Para permitir el uso simultáneo de los procesos de comunicación en un solo *host*, el módulo TCP proporciona una serie de direcciones o puertos dentro de cada *host*, que combinada con la dirección IP y la dirección local del host conforman lo que conocemos como *socket* [11], lo que permite identificar de forma única a cada conexión y de esta forma realizar múltiples conexiones. La asignación de los puertos a cada proceso se controla independientemente en cada *host*.

[11] Interfaz de conexión entre un proceso cliente y un proceso servidor. Es el punto final de comunicación.

Conexiones: TCP debe realizar un informe de estado para cada flujo de datos al iniciar una conexión. Una conexión se establece de forma única entre dos sockets que corresponden en ambos extremos. Cuando dos procesos desean comunicarse, sus módulos TCP establecen la conexión y la cierran al completarse. Para evitar inicializaciones erróneas de conexiones en sistemas de comunicación no fiables, se usa un mecanismo de números de secuencia basados en tiempos de reloj.

Prioridad y Seguridad: Cada usuario tiene la opción de indicar el nivel de prioridad y seguridad que desea para sus comunicaciones. Cuando no se especifican estas características se usan valores por defecto.

2.6.2 Protocolo IP (Protocolo de Internet)

El protocolo de Internet IP fue diseñado en un principio para la interconexión de redes. Proporciona los medios necesarios para transportar los bloques de datos (datagramas) de un origen a un destino, sin importar que los *hosts* se encuentren en la misma red, o haya otras redes entre ellos.

El datagrama IP se conforma de dos secciones, la primera es un encabezado que cuenta con una parte fija de 20 bytes y una parte opcional de longitud variable, la segunda es una parte de texto. El protocolo de internet trata a los datagramas como una entidad independiente sin ninguna relación con otro datagrama.

Este protocolo proporciona un servicio de mejor esfuerzo, es decir que hará lo mejor posible pero no garantiza la fiabilidad de datos entre los extremos, tampoco cuenta con un mecanismo de control de flujo por lo que no puede determinar si los datos llegaron a su destino, si fueron duplicados o si están dañados.

El protocolo de internet implementa dos funciones básicas:

Direccionamieto: Se hace uso de las direcciones que se encuentran en la cabecera para poder transmitir los datagramas hacia su destino. La elección de un camino para la transmisión se llama encaminamiento.

El encaminamiento se trata de la búsqueda de la mejor ruta posible mediante el uso de una tabla de encaminamiento en la que se especifica para cada posible red destino el siguiente dispositivo de encaminamiento al que se enviará el datagrama.

Fragmentación: Cuando es necesario el módulo IP hace uso de la cabecera para fragmentar o segmentar los datagramas en unidades más pequeñas para transmitirlos a redes que limitan el tamaño de los paquetes. Al llegar a su destino los datagramas son reensamblados.

Cada *host* involucrado en una red cuenta con un módulo IP, estos módulos tienen reglas similares que se encargan de interpretar las direcciones en las cabeceras y así ser capaces de fragmentar y reensamblar los datagramas. También tienen procedimientos para tomar decisiones de encaminamiento y otras funciones.

El protocolo de internet usa cuatro mecanismos esenciales para poder ofrecer sus servicios:

Tipo de servicio: Utilizado para indicar la calidad del servicio requerido, se basa en los parámetros que presentan los servicios seleccionados en las redes que conforman la Internet.

Tiempo de vida: Es el límite superior del periodo de vida de un datagrama. Esta marca es especificada por el remitente y se implementa un contador de saltos que reducirá el tiempo de vida cada vez que pase a través de un dispositivo de encaminamiento, si el tiempo de vida llega a cero antes de que el datagrama llegue a su destino, el datagrama se descarta.

Opciones: Proporcionan los recursos necesarios para marcas de tiempo, seguridad y encaminamiento especial.

Suma de control de cabecera: Sirve para proporcionar una verificación de que la información ha sido transmitida correctamente al procesar el datagrama. Si los datos contienen errores, al realizarse la suma de control de cabecera el datagrama será descartado ya que se encontrará una falla.

2.7 Servidor DHCP

El Protocolo de Configuración de Host Dinámico (DHCP - Dynamic Host Configuration Protocol) es utilizado para asignar automáticamente parámetros a un equipo cliente dentro de una red TCP/IP. El servidor DHCP centralizado proporcionará la configuración de red, que consiste en la dirección IP, la *máscara de subred*[12], la *puerta de enlace*[13] y los *servidores DNS*[14], cuando un cliente DHCP se comunique con él.

Este protocolo de red está basado en una arquitectura cliente/servidor en el que generalmente el servidor almacena en memoria una lista de direcciones IP en la que buscará y asignará la dirección disponible cuando el cliente la solicite.

El servidor DHCP puede configurarse para asignar direcciones IP en tres formas diferentes:
Asignación Automática: Designará permanentemente una dirección arbitraria al cliente.
Asignación Dinámica: Designará una dirección durante un determinado tiempo.
Asignación Estática: Designará una dirección reservada en función de la dirección física de la tarjeta de red del cliente.

2.7.1 Funcionamiento de un servidor DHCP

La interacción entre un cliente y un servidor se lleva a cabo mediante el uso de un sistema de comunicación conformado por 8 tipos de mensajes de difusión:
DHCPDISCOVER: Este mensaje es emitido por un cliente para localizar a los servidores disponibles.
DHCPOFFER: Es el mensaje de respuesta que envían los servidores activos ofreciendo al cliente sus parámetros de configuración.
DHCPREQUEST: El cliente elige un servidor y responde solicitando los parámetros de red, esta acción le informa a los otros servidores que rechaza sus ofertas.
DHCPACK: Mensaje que envía el servidor para confirmar los parámetros incluyendo la dirección de red.
DHCPNACK: Este mensaje es enviado al cliente por el servidor para informarle que la

[12] Conjunto de bits que permiten identificar la red y el host en una dirección IP.
[13] Dispositivo para interconectar redes, realiza la traducción necesaria cuando se usan protocolos diferentes.
[14] Encargados de traducir los nombres de dominio en sus respectivas direcciones IP.

dirección de red que solicita no es válida para la subred en la que se encuentra o que su *arrendamiento*[15] ha expirado.

DHCPDECLINE: El cliente envía este mensaje al servidor para informarle que esta usando la dirección.

DHCPRELEASE: Este mensaje es enviado por el cliente para informarle al servidor que no usará más la dirección IP y da por terminado su arriendo.

DHCPINFORM: Mensaje enviado por el cliente cuando ya está configurado, únicamente le pregunta al servidor sobre los parámetros de configuración local.

Cabe destacar que para lograr una comunicación entre cliente y servidor no son suficientes los mensajes anteriormente descritos, es necesario seguir una secuencia de eventos para iniciar el servicio DHCP:

El cliente DHCP emite un mensaje de descubrimiento (DHCPDISCOVER), en este mensaje se incluye la dirección MAC (Control de Acceso al Medio) que sirve como identificador único del cliente.

Los servidores que puedan brindar este servicio responden a la petición con el mensaje DHCPOFFER ofreciendo al cliente una dirección IP basándose en la interfaz de red y en la subred de donde proviene la petición, también se debe tener en consideración si la dirección IP está asociada específicamente a una dirección MAC o se le puede asignar una de las direcciones disponibles. Mientras esté en uso, la dirección asignada es reservada temporalmente por el servidor para evitar ofrecerla por segunda ocasión.

El cliente selecciona la mejor oferta y para confirmar los datos envía una respuesta (DHCPREQUEST) solicitando los parámetros de configuración del servidor que eligió, esta emisión le indica a los servidores restantes que el cliente ha seleccionado un servidor y pueden cancelar las reservaciones de las direcciones de red.

El servidor envía al cliente un mensaje de reconocimiento (DHCPACK) que contiene los parámetros de configuración de red y almacena en una base de datos la información del cliente y la IP asignada.

El cliente usa la información enviada por el servidor para configurar su interfaz de red. También debe supervisar el tiempo que usará la dirección IP, al transcurrir un tiempo

[15] Técnica utilizada para asignar direcciones IP, el servidor DHCP emite un préstamo por un tiempo determinado, al terminar el cliente debe solicitar una renovación o dejar de usar la dirección.

determinado éste envía al servidor un nuevo mensaje para renovar y aumentar el tiempo de permiso.

2.8 Sistema Operativo

El sistema operativo es un conjunto de programas lógicos encargados de administrar los dispositivos de hardware y los recursos de una computadora mediante la ejecución de procesos de control. Realiza operaciones ocultas de bajo nivel por lo que el usuario no se da cuenta de los complejos procedimientos que se ejecutan, además ofrece a los programas una interfaz sencilla para que el usuario logre comunicarse con el *hardware*. Su principal tarea es la repartición ordenada y controlado de los recursos entre el *hardware* y el *software* que compiten por obtenerlos.

La administración de los recursos del sistema se realiza apoyándose en dos tipos de comportamientos:

Multiplexaje en el tiempo: Este comportamiento se caracteriza por el hecho de que los programas o los usuarios toman turnos para poder hacer uso de los recursos. El sistema operativo decide de quien es el turno siguiente y el tiempo óptimo de uso.
Multiplexaje en el espacio: En este caso se realiza una repartición del recurso para cada cliente. El ejemplo más claro es cuando la memoria principal es asignada a diferentes programas en ejecución en lugar concentrarla en una sola tarea.

2.8.1 GNU/Linux

En 1971 Richard Stallman, estudiante del primer año de física en la Universidad de Harvard, se convirtió en un especialista de informática gracias a su trabajo en el laboratorio de Inteligencia Artificial del MIT. En ese entonces el código fuente de los programas se compartían libremente ya que en esa época no existía el concepto de *software* libre o *software* propietario.

Conforme pasaba el tiempo la industria del *software* se dio cuenta de que era un negocio rentable lo que originó que a principios de los 80's el *software* ya no fuera cooperativo si no propietario, las compañías obligaron a los usuarios a pagar licencias y a firmar acuerdos de "no revelar" para poder usarlo, y más importante aún, no se podía tener acceso al código fuente.

Esta situación fue la que orilló a Stallman a buscar otras alternativas, ya que consideraba al *software* propietario como antisocial, abandona el MIT y en 1983 inicia el proyecto GNU, agregando*:* "Cualquier usuario debe poder modificar un programa para ajustarlo a sus necesidades y cualquier usuario debe poder compartir el software, porque ayudarnos unos a otros es la base de la sociedad".

Este proyecto consistía en desarrollar un conjunto de aplicaciones y un sistema operativo que fueran completamente libres y compatibles con UNIX para su portabilidad. El nombre que se eligió fue GNU que significa GNU's Not Unix (GNU no es UNIX). Su primer logro fue el compilador de c llamado gcc, el cual sigue siendo de vital importancia para el desarrollo de *software* UNIX.

A principios de los 90's el sistema estaba casi terminado, solo faltaba un *kernel*[16], se inició el desarrollo de GNU Hurd, sin embargo hasta el día de hoy no está listo. Afortunadamente otro *kernel* estaba disponible: Linux.

En 1991 Linus Torvalds era un estudiante de segundo año de informática en la Universidad de Helsinki, se caracterizaba por ser un programador autodidacta. El 25 de agosto del mismo año, a los 21 años de edad, envía un correo al grupo de noticias de *MINIX*[17]:

"Estoy haciendo un sistema operativo (gratuito, solo un hobby, no será nada grande ni profesional como GNU) para clones AT 386(486). Llevo en ello desde abril y está empezando a estar listo. Me gustaría saber su opinión sobre las cosas que les gustan o disgustan en minix, ya que mi SO tiene algún parecido con él [...] Actualmente

[16] Software fundamental en un sistema operativo ya que es el encargado de administrar los recursos y dispositivos de la máquina mediante llamadas al sistema, también se encarga de gestionar la comunicación entre los programas y el hardware.

[17] Sistema Operativo desarrollado por el académico Andrews Tanenbaum para enseñar a sus alumnos el funcionamiento interno de un sistema operativo real, fue muy importante ya que su código fuente estaba disponible.

he portado bash(1.08) y gcc(1.40), y parece que las cosas funcionan. Esto implica que tendré algo práctico dentro de unos meses..."

Para mediados de septiembre fue lanzada la primera versión 0.01 de Linux, la comunidad lo descargó y envió sus modificaciones a Linus, incluso recibió un correo de parte de Tanenbaum donde pronosticaba su fracaso, esta situación no lo desanimó y siguió adelante con su proyecto.

Las nuevas versiones betas siguieron publicándose con las mejoras del sistema bajo una licencia propia de Torvalds en la cual se especificaba que el código fuente podía compartirse pero quedaba estrictamente prohibido el uso comercial, fue a principios de 1992 cuando Linus decidió adoptar la licencia GNU GPL (Licencia Pública General de GNU) para su distribución lo que permitía que cualquier persona tenía acceso al código fuente para utilizarlo, modificarlo o distribuirlo libremente. Esta decisión permitió que a mediados de 1992 la combinación de GNU/Linux resultara en un sistema operativo libre, completo y funcional.

Es importante mencionar que el desarrollo de GNU/Linux se debe en gran parte al apoyo de una gran comunidad de programadores y usuarios que aportan su tiempo y sus ideas.

2.8.2 Razones para usar GNU/Linux

Hay muchas razones para usar GNU/Linux, pero las más importantes y las que consideramos esenciales para el desarrollo de nuestro proyecto son:

Estabilidad y Confiabilidad: GNU/Linux se desarrolla basándose en la arquitectura UNIX, la cual ha sido probada y refinada durante más de 35 años demostrando ser muy eficaz, robusta y segura. Además se ha diseñado desde cero para crear un sistema operativo estable y resistente a los fallos de sistema, por lo que rara vez es necesario reiniciarlo.

Seguridad: GNU/Linux es prácticamente inmune a los virus, troyanos y gusanos ya que fue diseñado desde un comienzo con la seguridad en mente. Se trabaja con permisos de administración para proteger los principales archivos del sistema, es decir, se protege desde adentro y no con aplicaciones adicionales al sistema.

Flexibilidad: GNU/Linux nos da la libertad de configurar el sistema para adaptarlo a nuestras necesidades, ya que puede ser optimizado para estación de trabajo, para servidor o para su uso en una PC.

Libertad: Gracias a que GNU/Linux es distribuido bajo una licencia GPL tenemos la libertad de modificar, editar y redistribuir nuestro sistema. Podemos realizar modificaciones sencillas o cambiar complejas líneas de código para hacer que trabaje adecuándolo a nuestras necesidades.

Costo: No es necesario pagar por una licencia ya que la mayoría de las distribuciones de GNU/Linux son gratuitas, incluso puede descargarse de internet e instalarlo sin restricciones en cuantas máquinas se desee.