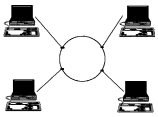
CAPÍTULO 1

REDES DE DATOS



1.1 Introducción a las redes

Se le llama red de computadoras al conjunto de elementos que interaccionan entre sí con el propósito de compartir recursos e intercambiar información. Se consideran elementos aquellos que sirven de propósito especial como lo son los nodos, las terminales, los servidores, las computadoras, entre otros.

Una de las razones por la cual es muy frecuente el uso de las redes es por la flexibilidad con la que se cuenta, ya que la forma de comunicarse con otra persona es más fácil y se presenta rapidez que se tiene al transferir cualquier documento vía internet.

Otra de las razones por la cual se incrementó el uso fue el gran ahorro económico que se obtuvo al compartir recursos tanto lógicos como físicos, permitiendo así un gran porcentaje de aceptación para el usuario general. Las redes se clasifican de acuerdo con su alcance geográfico y se muestra esta clasificación a continuación en la tabla 1.1.

Tabla 1.1 Clasificación de las redes

Tipo de red	Distancia	Lugares donde se utiliza
PAN (Personal Area Network – Red de Área Personal)	≤ 10 m.	Espacio personal (oficina, cubículo)
LAN (Local Area Network – Red de Área Local)	≤ 1 Km.	Escuelas, habitación, edificios, universidad
CAN (Campus Area Network - Red de Área de Campus)	≤ 10 Km.	Universidad, base militar
MAN (Metropolitan Area Network - Red de Área Metropolitana)	≤ 100 Km.	La ciudad
GAN (Global Area Network- Red de Área Global)	< 100 Km.	El Mundo (con retraso en la comunicación)
WAN (Wide Area Network – Red de Área Amplia)	≤ 1000 Km.	El mundo

Es importante mencionar que existen dos formas para que los equipos se interconecten, con base en ello se puede hacer una clasificación en redes cableadas y redes no cableadas:

a) Redes Cableadas (Guiadas). Son las que tienen la capacidad de transferir información de manera rápida, segura y efectiva, además de que su implementación es de menor costo que las redes inalámbricas.

Para llevar a cabo una conexión de este tipo se hace uso de medios de transmisión guiados o terrestres, entre ellos se encuentran los de tipo coaxial, par trenzado y fibra óptica.

El cable coaxial tiene un hilo de cobre en la parte central el cual está rodeado por una malla metálica y una cubierta protectora de plástico en forma cilíndrica. Una de las ventajas del cable coaxial es la resistencia a interferencias y atenuación. (Figura 1.1)

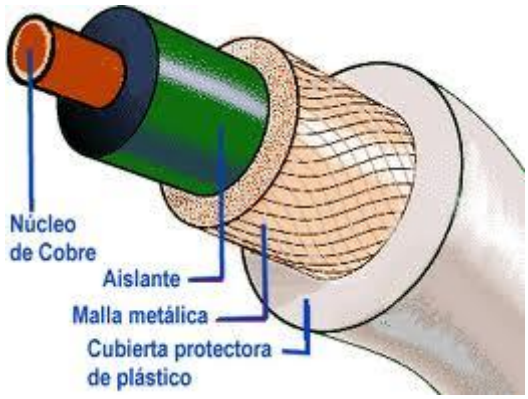


Figura 1.1 Cable Coaxial

El cable de par trenzado UTP (unshielded twisted pair- par trenzado no apantallado) está formado por un conductor interno protegido por una capa de polietileno y un grupo de pares de diferentes colores dentro de la capa se cuenta con tres pares. (Figura 1.2)

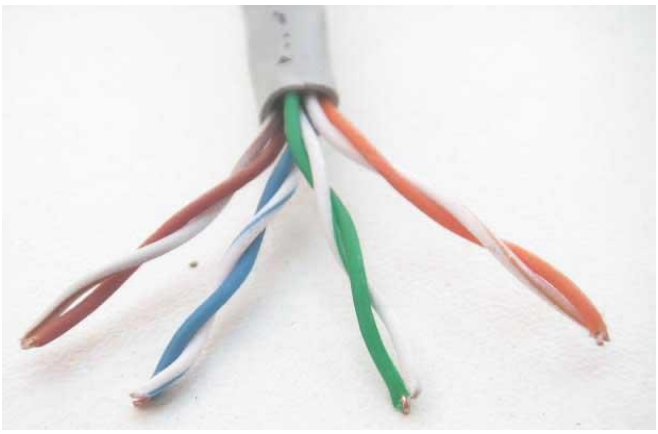


Figura 1.2 Cable UTP

Una de las ventajas de utilizar este cable es su bajo costo, además de que su uso es sencillo, sólo que tiene un problema el cual es la limitación para trabajar a largas distancias (máximo 100m). Este cable cuenta con diferentes categorías que van desde la categoria1 hasta la 7. Actualmente se utiliza en su mayoría el cable UTP categoría 5e que puede transmitir datos hasta de 100Mbps y consta de 4 pares trenzados de hilo de cobre. El cable UTP utiliza conectores RJ-45.

La fibra óptica es un hilo muy fino y por medio de estos hilos se envían pulsos de luz, es el mejor medio de transmisión ya que no hay problemas de interferencia, la velocidad con la que se trasmiten los datos es alta. (Figura 1.3)

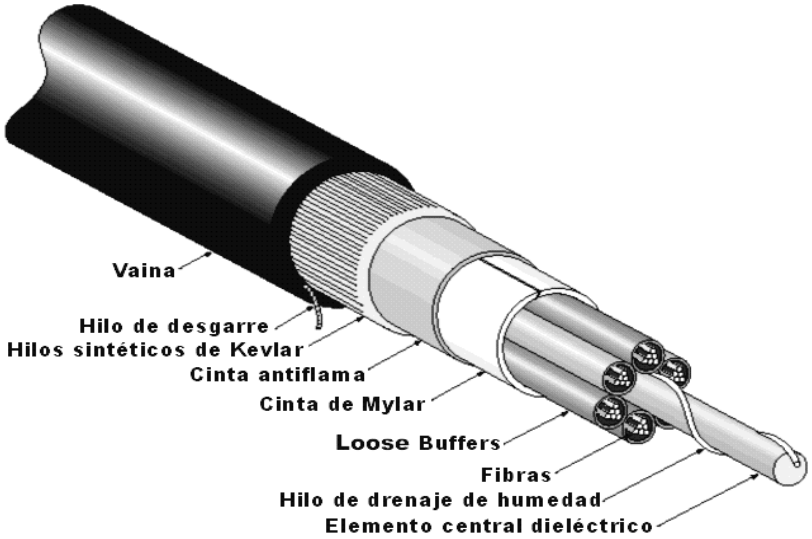


Figura 1.3 Cable de Fibra Óptica

Para realizar la comunicación se emplean fibras multimodo y monomodo, las multimodo se utilizan para distancias cortas que puede considerarse de hasta 5000 m. las fibras monomodo se emplean para distancias más largas.

La desventaja es su alto costo, además de que la fibra es muy frágil y se debe tener mucho cuidado en su utilización.

b) Redes no cableadas (Inalámbricas). Son aquellas que se comunican mediante ondas electromagnéticas y para la trasmisión y recepción se necesita una antena.

Entre las ventajas que tienen las redes inalámbricas es la rápida instalación de la red, la movilidad que se tiene, además del bajo costo en su mantenimiento.

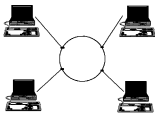
Los medios de transmisión se encargan de propagar las señales libremente a través del medio y se clasifican en 3 tipos: ondas de radio, microondas e infrarrojo. (Figura 1.4)

Figura 1.4 Medios de transmisión de una red inalámbrica

Las ondas de radio son ondas electromagnéticas de menor frecuencia ya que su rango se encuentra entre 3 a 30 Hz. Estas ondas son omnidireccionales por lo tanto no necesitarán de un aparato que se encargue de dirigir la señal ya que habrá varias antenas que la reciban.

En la transmisión por microondas la señal va viajando en línea recta entre las estaciones repetidoras hasta llegar a su destino, al llegar a éste, se amplifica la señal y se retransmite a otros puntos.

El infrarrojo se utiliza para una comunicación a corta distancia y tanto el transmisor como el receptor deben estar alineados directamente para lograr una



buena transmisión. La gran desventaja de este medio de transmisión es que no puede atravesar las paredes.

1.2 Topologías de las redes

La topología hace referencia a la forma de una red, muestra cómo los diferentes nodos se encuentran conectados entre sí y la forma de comunicarse. Las topologías pueden ser físicas o lógicas, existen diversos tipos:

a) Topología Bus

En esta topología las computadoras se encuentran conectadas en línea recta, es decir, todas las máquinas se encuentran conectadas a un cable en común, esto permite que se puedan comunicar directamente. El tipo de medio de transmisión (cable) que se utiliza en este tipo de conexión es el cable coaxial. La gran desventaja de este tipo de conexión es que la ruptura del cable hace que todos los nodos pierdan la comunicación.

A continuación se presentan dos tablas (1.2 y 1.3) con las características del cable coaxial delgado y del cable coaxial grueso, ambos permiten realizar con la que se hace una conexión tipo bus.

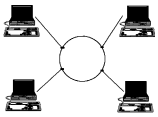


Tabla 1.2 Especificaciones del cable coaxial delgado

CABLE COAXIAL DELGADO RG-58	
Velocidad de operación	10 Mbps
Tipo de transmisión	Banda Base
Distancia máxima del segmento	185 m
Distancia mínima entre nodos	0.5 m
Diámetro del cable	¼ pulg
Material que se utiliza para la conexión	Conector BNC-T(del inglés Bayonet Neill-Concelman), Terminador

Tabla 1.3 Especificaciones del cable coaxial grueso

CABLE COAXIAL GRUESO RG-8	
Velocidad de operación	10 Mbps
Tipo de transmisión	Banda Base
Distancia máxima del segmento	500 m.
Distancia mínima entre nodos	2.5 m
Diámetro del cable	½ pulg
Material que se utiliza para la conexión	Transceiver tipo vampiro, terminador

La topología tipo bus emplea el cable coaxial delgado o grueso y puede observarse en las figuras 1.5 y 1.6

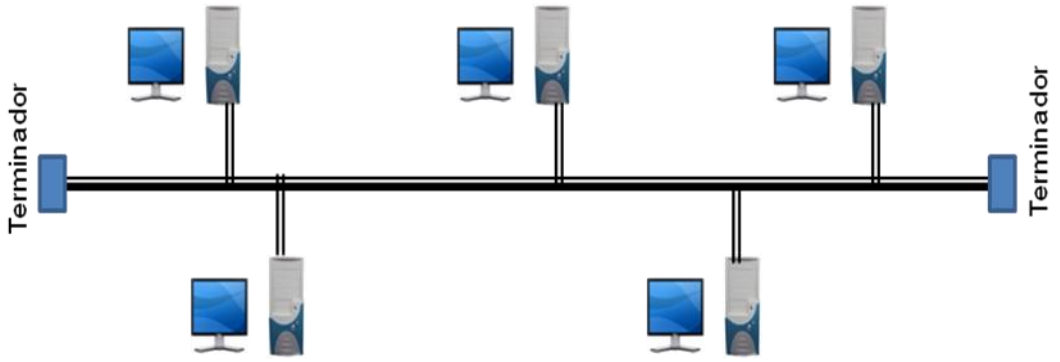


Figura 1.5 Topología en bus con cable coaxial delgado

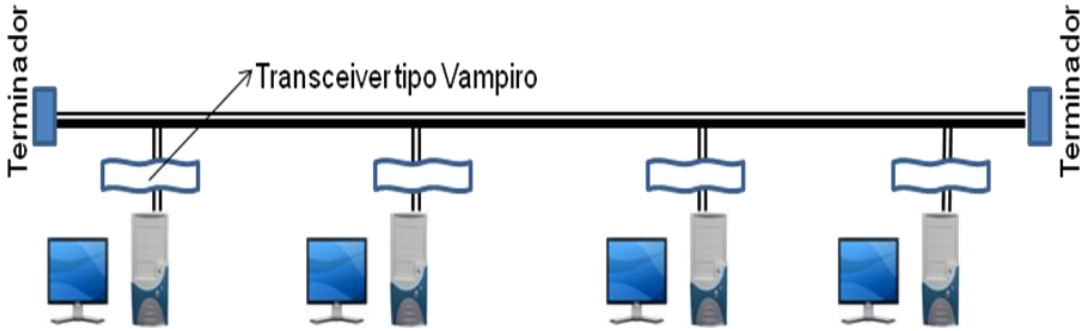
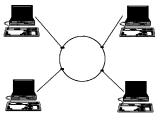


Figura 1.6 Topología en bus con cable coaxial grueso

Una de las ventajas de esta topología es que todos los dispositivos de la red pueden verse entre sí y compartir la información de manera que puede simularse que ésta se encuentra residente de manera local en el equipo que la solicita, otra gran ventaja es que se permite conectar un gran número de



equipos. La desventaja es que al compartir la información, como sólo se utiliza un canal de comunicación, esto provoca problemas de tráfico y colisiones.

b) Topología Anillo

Este tipo de topología se compone de un solo anillo cerrado donde los dispositivos se conectan directamente entre sí por medio de cables, la diferencia que se tiene con la topología bus es que las puntas no están conectadas a un terminador. Las ventajas que se observan en esta topología son las siguientes:

- Se tiene un acceso equitativo para todas las computadoras.
- El rendimiento del sistema no se altera demasiado cuando muchos usuarios están utilizando la red.

La desventaja de este tipo de conexión es que al cortar la cadena se interrumpe la conexión o si existe alguna distorsión afecta a toda la red, La figura 1.7 muestra cómo es la conexión tipo anillo.

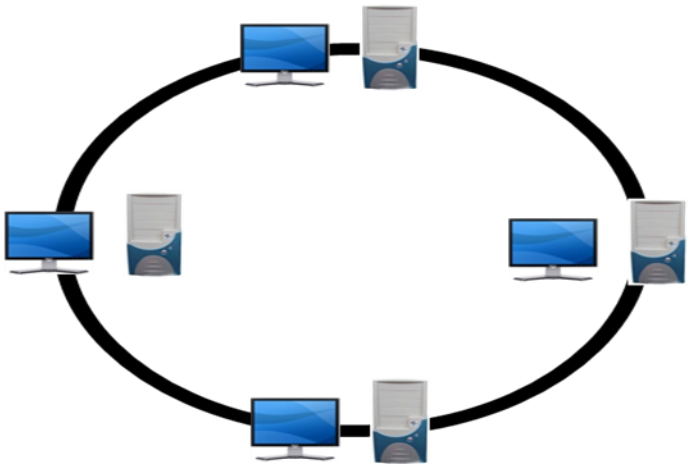


Figura 1.7 Topología en Anillo

c) Topología Estrella.

En este tipo de topología los dispositivos se encuentran conectados a un concentrador (hub) o conmutador (switch).

La ventaja de este tipo de conexión es que si un cable falla no afecta a los demás nodos ya que están conectados mediante un concentrador y sólo falla el equipo del cable dañado, otra ventaja es la administración y monitoreo centralizado.

Entre las desventajas se puede encontrar el alto costo en el cableado que se hace, así como las conexiones que se utilizan y en caso de que el concentrador presente alguna falla, la red queda inutilizable. (Figura 1.8)

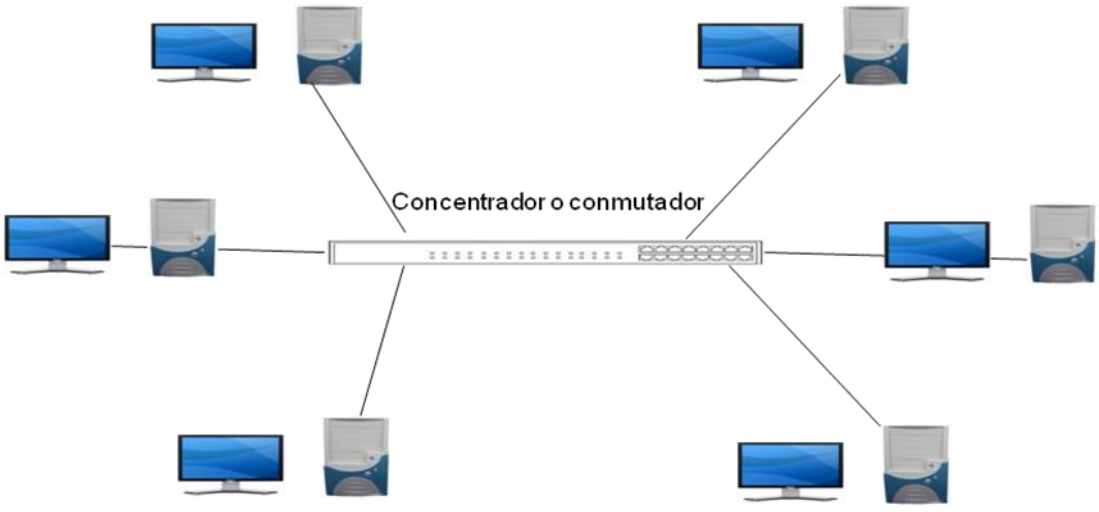


Figura 1.8 Topología en Estrella

d) Topología Malla

En esta topología cada nodo está conectado a todos los nodos, por lo que la comunicación entre un equipo y otro es de manera eficiente debido a que se cuenta con varios enlaces disponibles. Como ventaja es posible mencionar que si uno de los cables falla, la comunicación no se pierde, pues habrá otros cables disponibles para ese equipo, otra ventaja es el grado de confiabilidad, pues se tiene independencia en cada uno de los equipos conectados aunque estén conectados todos entre sí.

La gran desventaja es la parte económica, ya que conlleva un gasto enorme comprar demasiado cable para conectar todos los equipos. Otra de las desventajas que se tiene es el grado de complejidad en la realización de este tipo de conexión. La figura 1.9 muestra cómo es una topología malla.

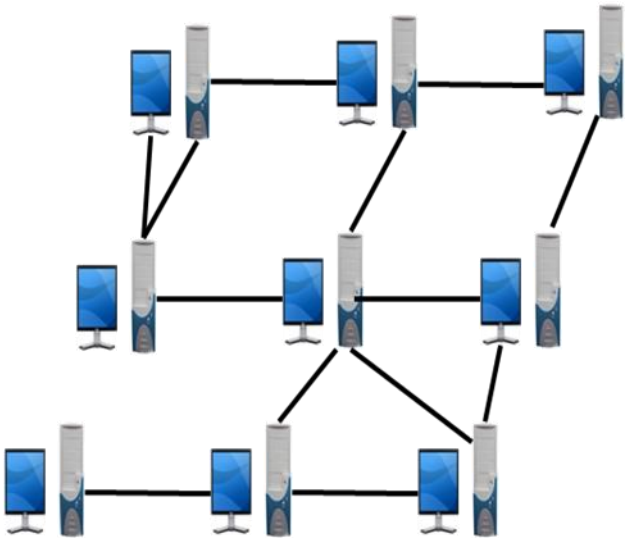
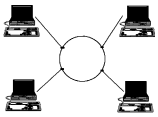


Figura 1.9 Topología Malla



e) Topología Híbrida

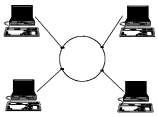
El término híbrido describe que está formada con diferentes protocolos, sistemas operativos y distintas plataformas, en este caso esta topología indica que está formada mediante la combinación de topologías básicas.

1.3 Estándares de las redes

Los estándares de las redes se realizan por medio del comité 802 del IEEE (Institute of Electrical and Electronic Engineers- Instituto de Ingenieros Eléctricos y Electrónicos) donde se definen los estándares para las redes LAN (Local Area Network – Redes de Área Local). La mayoría de los estándares se desarrollaron en la época de los 80 cuando apenas comenzaban a surgir las redes en los equipos de cómputo y telecomunicaciones, fue un desarrollo impresionante para todo el mundo, algunas empresas e instituciones gubernamentales de los países de primer mundo ya tenían esta tecnología, sin embargo, era muy caro el servicio de las telecomunicaciones y la instalación de las redes LAN y sus variantes en cuestión de tecnología en redes WLAN.

Dentro de los estándares de las redes de área local que fueron definidas por el comité 802, surgieron las diferentes categorías de las especificaciones 802 por su avance tecnológico y crecimiento de los servicios de Internet y telefonía móvil.

El comité 802 clasifica en 11 categorías los avances de los estándares, esto se observa a continuación:



a) Definición internacional de redes (802.1)

Establece los estándares de interconexión relacionada con la gestión de redes por IEEE y el modelo de referencia para la interconexión de sistemas abiertos (OSI – Open Systems Interconennection), de la Organización Internacional de Estándares (ISO - Internacional Standards Organization). El comité definió las direcciones para las estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única.

b) Control de enlaces lógicos (802.2)

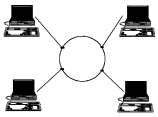
Se define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles: Los niveles LLC y MAC. El LLC (Logical Link Control - Control de Enlace Lógico) asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación y la MAC (Media Access Control - Control de Acceso al Medio) provee la dirección física de red de un dispositivo.

c) Redes CSMA/CD (Carrier Sense Multiple Access / Collision Detection – Acceso Múltiple con Detección de Portadora y Detección de Colisiones). (802.3)

El estándar 802.3 define cómo opera el método de acceso múltiple con detección de colisiones sobre varios medios. Este estándar define la conexión de redes sobre el cable coaxial, cable de par trenzado y medios de fibra óptica.

d) Redes token bus (802.4)

El estándar 802.4 define el esquema de red de amplios anchos de banda en la Industria, también se deriva del MAP (Manufacturing Automation Protocol - Protocolo de Automatización de Manufactura). Los tokens son pasados en orden lógico basado en la dirección del nodo, pero este orden puede no relacionarse con la posición física del nodo como se hace en una red token ring.



e) Redes token ring (802.5)

El estándar 802.5 de las redes token ring es también llamado ANSI (American National Standards Institute – Instituto Nacional de Estándares Norteamericanos)/IEEE 802.5, se creó en 1985 en donde se definieron los protocolos de acceso, cableado e interfaz para las LAN Token Ring, este estándar lo hizo popular IBM para el método de acceso de paso de tokens y físicamente es una conexión con topología estrella, pero lógicamente forma un anillo.

f) MAN (Metropolitan Area Network - Redes de Área Metropolitana) (802.6)

El estándar 802.6 trata de redes de área metropolitana definidas como redes de datos diseñadas para poblaciones o ciudades. Se define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado DQDB (Distributed Queued Dual Bus - Bus Dual de Cola Distribuida).

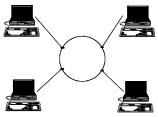
El DQDB es una red repetidora que conmuta celdas de longitud fija de 53 bytes; por lo consiguiente, es compatible con el ancho de banda ISDN (Integrated Services Digital Network - Red Digital de Servicios Integrados) y ATM (Asynchronous Transfer Mode - Modo de Transferencia Asíncrona)

g) Grupo asesor técnico de ancho de banda (802.7)

Este comité brinda consejos técnicos a otros subcomités en técnicas sobre anchos de banda en redes.

h) Grupo asesor técnico de fibra óptica (802.8)

Este consejo brinda asesoría de redes por fibra óptica a otros subcomités como una alternativa a las redes basadas en cable de cobre.



i) Redes integradas de datos y sonido (802.9)

Define la integración de tráfico de sonido, datos y video para las LAN, también existe una especificación llamada IVD (Integrated Voice Data - Datos y Voz Integrados), este servicio provee un flujo multiplexado que pueda llevar canales de información de datos y sonido conectando dos estaciones sobre un cable de cobre o un par trenzado.

j) Grupo asesor técnico de seguridad en redes (802.10)

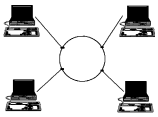
Se trabaja en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y cifrado para redes LAN Y WLAN.

k) Redes inalámbricas (802.11)[1]

Conocido también como WIFI, es una familia de estándares, especificaciones o protocolos de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y enlace de datos), especificando las normas de funcionamiento en una WLAN.

Se han desarrollado diversas especificaciones en esta familia debido a que han surgido nuevas necesidades para utilizar los medios más adecuados para lograr la implementación de una red inalámbrica en cualquier lugar.

[1] Para mayor información ver el apéndice A



1.4 Protocolos utilizados en las redes

Un protocolo es un conjunto de reglas que permite la comunicación entre ambos procesos que se ejecutan en diferentes equipos de cómputo, es un conjunto de reglas y procedimientos que se deben respetar para poder enviar y recibir los datos a través de la red.

Los protocolos son los encargados de establecer la forma en que se enviarán los paquetes de información considerando las necesidades de las organizaciones, éstos acoplan la información para su transmisión entre redes con diferentes protocolos, de esta manera se garantiza la comunicación entre redes, logrando así que los datos puedan llegar a su destino.

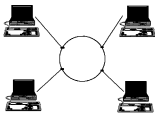
Los protocolos se pueden clasificar en protocolos orientados a la conexión y protocolos no orientados a la conexión.

a) Protocolos orientados a la conexión

Permiten el control de la transmisión de datos durante una comunicación establecida entre 2 equipos de cómputo. El equipo receptor se encarga de enviar los datos de recepción durante la comunicación y el equipo remitente es el responsable de validar los datos que está enviando. La lista de protocolos orientados a la conexión son: TCP, FRAME RELAY Y ATM.

Las características de los protocolos orientados a la conexión son:

1) Una red orientada a conexión cuida bastante los datos del usuario.



2) Exige una confirmación explícita de que se ha podido establecer esa conexión.

3) Si no se cumple lo anterior, la red informa al usuario solicitante que no ha podido establecer esa conexión.

4) Se intenta asegurar que los datos no se pierdan en la red.

b) Protocolos no orientados a la conexión

Método de comunicación por el cual el equipo remitente envía datos sin avisarle al equipo receptor, esto indica que recibe los datos sin enviar una notificación de recepción al remitente. Los protocolos no orientados a la conexión son: IP, UDP, ICMP, IPX Y TIPC.

Las características de los protocolos no orientados a la conexión son:

1) Las redes no orientadas a conexión pasan directamente del estado libre al modo de transferencia de datos.

2) Las redes no ofrecen confirmaciones, control de flujo, ni recuperación de errores aplicables a la red.

3) El costo de una red no orientada a conexión es mucho menor.

Las principales implementaciones en los protocolos definen que únicamente se deben comunicar los equipos, es decir, indican el formato y la propia secuencia de datos que van a intercambiar, por el contrario, un protocolo no define cómo se debe programar el software para que sea compatible con el protocolo adecuado dependiendo del sistema operativo y el hardware.

Las especificaciones de los protocolos nunca son exhaustivas, es común que las implementaciones estén sujetas a una determinada interpretación de las especificaciones, lo cual genera ciertas implementaciones; incompatibilidad o fallas de seguridad, por las características propias de cada protocolo conviene mencionar éstos a continuación: educativa.

a) HTTP

Desde 1990 se creó el protocolo HTTP (Hyper Text Transfer Protocol - Protocolo de Transferencia de Hipertexto), es el protocolo más utilizado en el servicio de Internet.

El principal objetivo de este protocolo es permitir la transferencia de archivos entre un navegador cliente y un servidor web localizado mediante una cadena de caracteres denominada dirección URL , el modelo del protocolo se muestra en el siguiente diagrama (Figura 1.10)

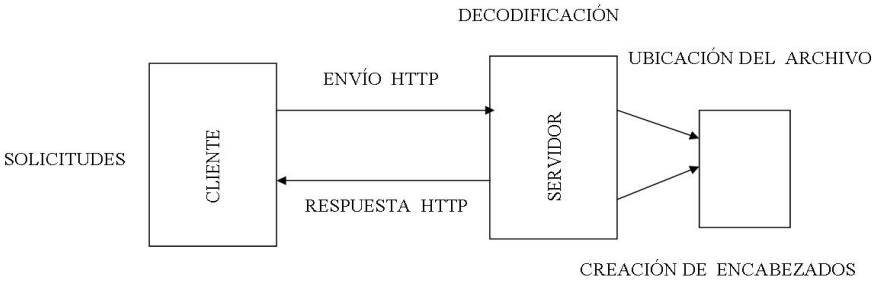
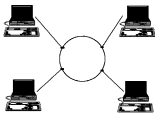


Figura 1.10 Modelo del protocolo HTTP



La manera de realizar una solicitud mediante el protocolo HTTP es un conjunto de líneas que el navegador envía al servidor con los siguientes puntos:

1. **Una línea de solicitud**. Es una línea que especifica el tipo de documento que se quiere solicitar, el método que se aplica y la versión del protocolo utilizado. La dirección está formada por tres elementos que deben estar separados por un espacio.
2. **Los campos del encabezado de solicitud**. Es un conjunto de líneas que permite aportar información a la solicitud y al cliente (navegador, sistema operativo, etcétera).Cada línea está formada por un nombre que describe el tipo de encabezado.
3. **El cuerpo de la solicitud**. Es un conjunto de líneas opcionales que deben estar separadas por una línea en blanco. Por ejemplo, permiten que se envíen datos mediante un comando POST durante la transmisión de datos al servidor.

b) FTP

El protocolo FTP (File Transfer Protocol – Protocolo de transferencia de archivos), como su nombre lo indica, es un protocolo para transferir archivos. El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP. El principal objetivo del protocolo FTP es permitir que los equipos remotos puedan compartir archivos y también permitir la comunicación entre los sistemas de archivos del equipo del cliente y del servidor.

El protocolo FTP está dentro del modelo cliente - servidor, es decir, cuando una aplicación cliente FTP inicia una conexión a un servidor FTP, abre el puerto 21 en el servidor conocido como el puerto de comandos. Se utiliza este puerto para

arrojar todos los comandos al servidor y para cualquier petición de datos desde el servidor se devuelve al cliente a través del puerto de datos. El número de puerto varía dependiendo si el cliente solicita los datos en modo activo o en modo pasivo. (Figura 1.11)

- **Modo Activo**: El modo activo es el método original utilizado por el protocolo FTP para la transferencia de datos a la aplicación cliente. Cuando el cliente FTP inicia una transferencia de datos, el servidor abre una conexión desde el puerto 20 en el servidor para la dirección IP y un puerto aleatorio sin privilegios especificado por el cliente.

- **Modo Pasivo**: La aplicación FTP cliente es la que inicia el modo pasivo de la misma forma que el modo activo. El cliente FTP indica que desea acceder a los datos en modo pasivo y el servidor proporciona la dirección IP y el puerto aleatorio sin privilegios en el servidor y luego el cliente se conecta al puerto en el servidor y descarga la información requerida.

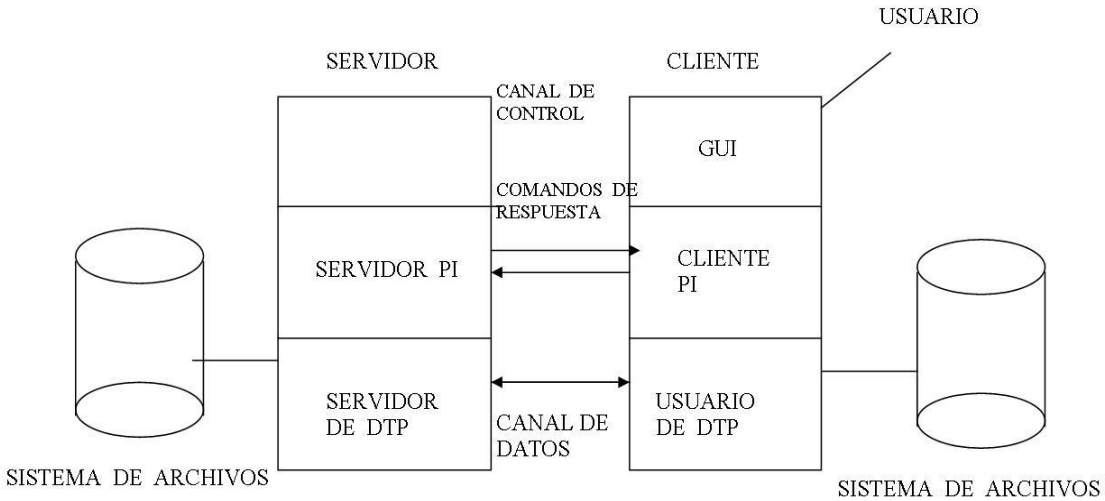
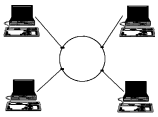


Figura 1.11 Modelo del protocolo FTP



Donde:

- DTP (Proceso de Transferencia de Datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina servidor de DTP y del lado del cliente se denomina usuario DTP.

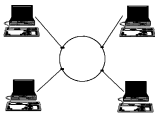
- PI (Intérprete de Protocolo) es el que interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control.

- GUI(Interfaz Gráfica de Usuario) el usuario puede interactuar directamente con el proceso servidor FTP y el diseño del protocolo está orientado a la utilización de los lenguajes autómatas.

c) ARP

El protocolo ARP (Address Resolution Protocol - Protocolo de Resolución de Dirección) tiene un papel clave entre los protocolos de la capa de Internet del modelo TCP/IP, ya que le permite que se conozca la dirección física de una tarjeta de interfaz de red asociada a una dirección IP.

La direcciones físicas se puedan asociar con las direcciones lógicas, el protocolo ARP se comunica con los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda de direcciones lógicas y físicas en una memoria caché. Si la dirección requerida no se encuentra en la tabla, entonces el protocolo ARP envía una solicitud a la red. Si todos los equipos en la red comparan esta dirección lógica con la suya, entonces se identificará con esta dirección al equipo que le confirme al protocolo ARP.



Existe otra variante del protocolo, éste es llamado RARP que consiste en un tipo de directorio inverso de direcciones lógicas y físicas. En realidad el protocolo RARP se usa esencialmente para las estaciones de trabajo sin discos duros que desean conocer su dirección física.

El protocolo RARP (Protocolo de Resolución de Dirección Inversa) es de un tipo de directorio inverso de direcciones lógicas y físicas. Este tipo de protocolo le permite a la estación de trabajo investigar su dirección IP desde una tabla de búsqueda entre las direcciones MAC y las direcciones IP alojadas en la misma red de área local (LAN).

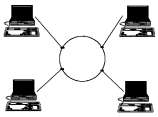
d) ICMP

El protocolo ICMP (Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet) permite administrar información relacionada con errores de los equipos en la red. El ICMP no permite corregir los errores sólo los notifica a los protocolos de capas cercanas. Por lo tanto, el protocolo ICMP es empleado por todos los routers para indicar un error.

e) IP

El protocolo IP (Internet Protocol - Protocolo de Internet) utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro bytes o cuatro números enteros decimales entre 0 y 255, están escritas en el formato xxx.xxx.xxx.xxx, por ejemplo, 146.153.205.26 es una dirección IP en formato técnico.

Los equipos de cómputo de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva. La organización ICANN (Internet Corporation for Assigned Names and Numbers – Corporación de Internet para la Asignación de Nombres y Números) es la responsable de asignar direcciones públicas de IP, es decir, direcciones IP para



los equipos de cómputo conectados directamente a la red pública de Internet, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

Existen diferentes clases de redes con el protocolo IP y se clasifican de acuerdo con la cantidad de bytes que representan a la red, las clases se muestran a continuación:

1. Clase A

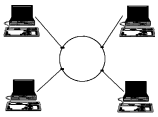
Es una dirección IP de clase A cuando el primer byte representa a la red (considerando los bytes de izquierda a derecha). El bit más importante es el primer bit a la izquierda que está en cero, lo que significa que hay 2^7posibles redes, es decir, 128, considerando el rango del primer byte de 0000001 a 01111111, en decimal y con el formato técnico para representar las direcciones IP se tiene las redes disponibles de clase A que van desde 1.0.0.0 a 127.0.0.0.

2. Clase B

En una dirección IP de clase B, los primeros dos bytes representan a la red. Los primeros dos bits siempre son 10; esto significa que existen 2^{14} posibles redes, es decir, 16384 redes posibles, considerando el rango de los primeros dos bytes de 10000000 00000000 a 10111111 11111111, en decimal y con el formato técnico para representar las direcciones IP se tiene que las redes disponibles de la clase B van de 128.0.0.0 a 191.255.0.0.

3. Clase C

En una dirección IP de clase C, los primeros tres bytes representan a la red. Los primeros tres bits siempre son 110; esto significa que hay 2^{21} posibles redes, es decir,2097152, considerando el rango de los primeros tres bytes de 11000000 00000000 00000000 a 11011111 11111111 11111111, en decimal y con el



formato técnico para representar las direcciones IP se tiene que las redes disponibles de la clase C van desde 192.0.0.0 a 223.255.255.0

4. Clase D

Se caracterizan porque su dirección comienza con la secuencia de bits 1110 y corresponden a las direcciones desde la 224.0.0.0 a la 239.255.255.255. Estas direcciones reciben el nombre de multicast, es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Un paquete dirigido a una dirección multicast es entregado a todas las máquinas que componen al grupo.

5. Clase E

Se caracterizan porque su dirección comienza con la secuencia 1111 y van desde la 240.0.0.0 hasta la 255.255.255.255. Son direcciones especiales reservadas por la IANA (la Autoridad Administradora de Dominios) y sólo está asignada la 255.255.255.255 que corresponde a todas las máquinas conectadas a un soporte físico.

El principal objetivo de dividir las direcciones IP en las clases comerciales A, B y C es facilitar la búsqueda de un equipo en la red, la asignación de una dirección IP se realiza de acuerdo con el tamaño de la red (Tabla 1.4)

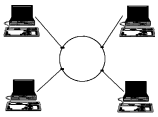


Tabla 1.4 Clasificación de las Distintas Clases de Redes

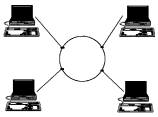
CLASE	CANTIDAD DE REDES POSIBLES	CANTIDAD MÁXIMA DE EQUIPOS EN CADA RED
A	126	16777214
B	16384	65534
C	2097152	254

f) TCP

TCP (Transmission Control Protocol - Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo OSI, es un protocolo orientado a la conexión que proporciona fiabilidad, control de flujo y recuperación de errores; protocolo punto a punto que suministra una conexión lógica entre pares de procesos, identificados cada uno de ellos por un socket, utilizando los números de puertos de éstos como comunicación con los procesos de nivel superior. El protocolo TCP es un protocolo orientado a la conexión, es decir, permite que dos computadoras estén en comunicación y tengan un control de estado de la transmisión.

Las principales características que tiene el protocolo TCP son las siguientes:

- TCP permite colocar los datagramas nuevamente en orden cuando provienen del protocolo IP.
- TCP permite el monitoreo del flujo de los datos y así evita la saturación de la red.



- TCP permite que los datos se formen en segmentos de longitud variada para entregarlos al protocolo IP.

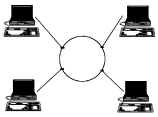
El principal objetivo del protocolo TCP está en las aplicaciones que pueden comunicarse en forma segura con el sistema de archivos que manejan al protocolo TCP independientemente de las capas inferiores. El protocolo TCP garantiza la transferencia de datos confiable.

La conexión que se establece en el protocolo TCP entre las dos aplicaciones a menudo se realiza siguiendo el siguiente esquema:

- Los puertos TCP deben estar abiertos.
- La aplicación en el servidor es pasiva, es decir, que la aplicación escucha y espera una conexión.
- La aplicación del cliente realiza un pedido de conexión al servidor

El TCP debe realizar también el control de flujo. Para ello el módulo receptor va informando al módulo emisor de la cantidad de octetos que puede recibir sin problemas en cada lapso de tiempo, mediante un mecanismo llamado ventana deslizante. A fin de utilizar más eficientemente los recursos disponibles TCP ofrece la posibilidad de múltiple acción entre distintos procesos de usuario, transmisión simultánea y la posibilidad de especificar niveles de seguridad o prioridad para las comunicaciones que asegura que la conexión no se cierra hasta no haber recibido confirmación de la recepción de todos los datos enviados.

La estructura general del encabezado del protocolo TCP se observa en la figura 1.12



<table>
<tr><td colspan="8">Puerto de origen (16</td><td colspan="2">Puerto de destino (16 bit)</td></tr>
<tr><td colspan="10">Número de orden (32 bit)</td></tr>
<tr><td colspan="10">Número de reconocimiento (32 bit)</td></tr>
<tr><td>Desplazamiento de los datos (4 bit)</td><td>Reservado (6 bit)</td><td>U R G</td><td>A C K</td><td>P S H</td><td>R S T</td><td>S Y N</td><td>F I N</td><td colspan="2">Ventana (16 bit)</td></tr>
<tr><td colspan="8">Código de verificación (16 bit)</td><td colspan="2">Puntero a datos urgentes (16 bit)</td></tr>
<tr><td colspan="7">Opciones (Variable)</td><td colspan="3">Relleno</td></tr>
<tr><td colspan="10">Datos (Variable)</td></tr>
</table>

Figura 1.12 Estructura del encabezado del protocolo TCP

Donde:

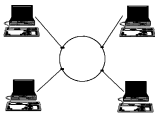
1. Puerto de origen: Identifica al proceso de un puerto de origen.

2. Puerto de destino: Identifica al proceso de un puerto de destino.

3. Número de orden: Número de orden del byte que identifica la posición inicial de los datos del segmento con respecto al flujo de bytes original del emisor.

4. Número de Reconocimiento: Indica el número de orden del byte que el receptor espera.

5. Desplazamiento de los datos: Indica la longitud de la cabecera de TCP medida en palabras de 32 bits.



6. Reservado: Campo reservado para el uso futuro que debe llevar todos sus bits a 0.

7. Banderas: Los siguientes seis campos son indicadores para solicitar servicios o marcar la validez de otros campos de la cabecera.

8. Ventana: Indica el número de octetos que el receptor podría aceptar.

9. Código de verificación: Se usa para verificar la corrección de los datos contenidos en el segmento incluida la cabecera.

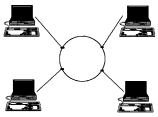
10. Puntero a datos urgentes: Este campo, válido sólo si el URG está a 1, indica los datos considerados urgentes que cada implementación tratará de manera diferente.

11. Opciones: Un campo para implementación de opciones que funciona de manera similar a como lo hace el campo opciones del datagrama IP. Cada opción tiene tres campos, un octeto que contiene el código de opción, un campo que indica la longitud de la opción y el tercer campo que incluye los valores propios de la opción. Las tres opciones disponibles actualmente son: fin de lista de opciones, código 0, sin operación, código 1, y longitud máxima del segmento, código 2.

12. Relleno: Relleno de bit a cero para completar palabra de 32 bit.

g) UDP

UDP (User Datagram Protocol - Protocolo de Datagrama de Usuario) es un protocolo del modelo OSI. Este protocolo es muy simple, ya que no proporciona



detección de errores, a continuación se muestra encabezado del segmento UDP en la Figura 1.13

Puerto de origen (16 bits)	Puerto de destino (16 bits)
Longitud total (16 bits)	Suma de comprobación del encabezado (16 bits)
Datos (Longitud variable)	

Figura 1.13 El encabezado del segmento UDP

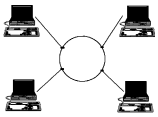
Donde:

1. Puerto de origen: Es el número de puerto relacionado con la aplicación del remitente del segmento UDP.

2. Puerto de destino: Este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

3. Longitud: Este campo especifica la longitud total del segmento con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4^{16} bits, por lo tanto, la longitud del campo es necesariamente superior o igual a 8 bytes.

4. Suma de comprobación: Es una suma de comprobación realizada de manera tal que permite controlar la integridad del segmento.



h) SMTP

SMTP (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión de punto a punto. Este protocolo funciona en línea, encapsulado en una trama TCP/IP. El correo se envía directamente al servidor de correo del destinatario.

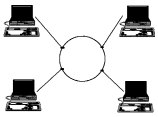
El protocolo SMTP funciona con comandos de texto enviando al servidor SMTP vía el puerto 25 de manera predeterminada. A cada comando enviando por el cliente le sigue una respuesta del servidor SMTP compuesta por un número y un mensaje descriptivo.

i) POP

El protocolo POP (Post Office Protocol - Protocolo de Oficina de Correos), permite descargar el correo electrónico desde un servidor remoto. Es adecuado para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar los correos electrónicos recibidos sin que estar conectados.

Existen dos versiones principales de este protocolo, POP2 y POP3, y se encuentran asignadas a los puertos 109 y 110 respectivamente, para establecer una conexión a un servidor POP2 el cliente de correo abre una conexión TCP en el puerto 109 del servidor. Cuando la conexión se ha establecido, el servidor POP2 envía al cliente POP2 una invitación y después las dos computadoras se envían entre sí otras órdenes y respuestas que se especifican en el protocolo. Como parte de esta comunicación, al cliente POP2 se le pide que se autentique, el nombre de usuario y la contraseña del usuario se envían al servidor POP2. Si la autenticación es correcta, el cliente POP2 pasa al estado de transacción.

El POP3 está diseñado para recibir correo, no para enviarlo. La mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de



manera tal que un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

j) TELNET

Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente en el sistema (compuesto de una pantalla y un teclado) con el intérprete de comandos en la parte del servidor.

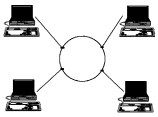
El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII, éste se codifica en 8 bits, entre los cuales se encuentran secuencias de verificación del Telnet.

El protocolo Telnet se basa en tres conceptos básicos:

- El paradigma terminal virtual de red NVT (Network Virtual Terminal - Terminal Virtual de Red).
- El principio de opciones negociadas.
- Las reglas de negociación.

Las especificaciones de Telnet no mencionan la autenticación por parte del protocolo, éste no es un protocolo de transferencia de datos seguro ya que los datos que transmite circulan en la red como texto sin codificar. Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funcione como servidor, el puerto que utiliza es el 23.

El protocolo Telnet consiste en crear una abstracción de la terminal que permita a cualquier host de cliente a servidor comunicarse con otro host sin conocer sus características



1.5 Modelo OSI

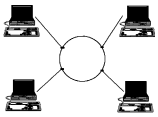
Modelo de Interconexión de Sistemas Abiertos por sus siglas en inglés (Open System Interconnection). Este Modelo se vio impulsado por la ISO (International Organization for Standardization - Organización Internacional para la Normalización) y el motivo de éste es una definición de procedimientos estandarizados que permitan la interconexión de información entre usuarios.

Cabe aclarar que el modelo OSI no trata sobre ninguna implantación tecnológica, sólo muestra la forma de interoperar sistemas abiertos.

El modelo OSI está formado por 7 capas (Ver figura 1.10)

7.- Aplicación
6.- Presentación
5.- Sesión
4.- Transporte
3. Red
2.- Enlace
1.- Física

Figura 1.10 Capas del Modelo OSI



1. Capa Física

Esta capa es la que se ocupa de la interfaz física entre los dispositivos, entre otras funciones, las cuales son la transmisión de los bits a lo largo del canal de comunicación.

Las características más importantes de esta capa son el aspecto mecánico que está relacionado con la especificación del conector que transmite las señales a través de los conductores.

La siguiente característica es la eléctrica en la cual se especifica cómo se representan los bits.

Entre los medios de transmisión se observan dos tipos:

- Medios guiados: cable coaxial, cable de par trenzado no apantallado (UTP), fibra óptica.
- Medios no guiados: radio, infrarrojos, microondas, láser, satelital.

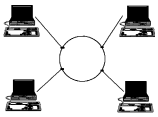
En los medios guiados la trasmisión es por medio de impulsos eléctricos, mientras que los medios no guiados emplean la transmisión por impulsos electromagnéticos.

2.- Capa de Enlace

Esta capa se encarga del direccionamiento físico, de la detección y control de errores, esto quiere decir que el emisor segmenta la información en tramas de datos y las transmite.

El Instituto de Ingenieros Eléctricos Electrónicos (IEEE) subdividió la capa de enlace en dos subcapas:

- *Control de Enlace Lógico (LLC).* Define cómo serán transferidos los datos sobre el medio físico, además de manejar el control de errores de transmisión, regular el



control de flujo de las tramas y encargada del direccionamiento de la subcapa MAC. En esta subcapa se ofrecen servicios orientados a conexión(garantizar la entrega de los datos) y los servicios orientados a no conexión (los datos no pueden ser entregados en su totalidad por no haber una conexión al momento)

- *Control de Acceso al Medio(MAC).* Se encarga de controlar el acceso al medio físico que los dispositivos comparten al mismo canal de comunicación, agregar nodo fuente y nodo destino a cada una de las tramas que se transmiten, detección y corrección de errores de transmisión y descartar tramas duplicadas o tramas que tienen fallas.

3.- Capa de Red

En esta capa el principal objetivo es hacer que los datos lleguen desde el origen hasta el destino, todo esto se hace mediante un encaminador comúnmente llamado router. Esto indica que se busca la mejor ruta para que el paquete llegue a su destino

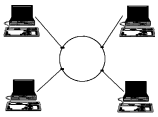
Esta capa también cuenta con el control de congestión, pues en un momento determinado existen demasiados paquetes en la subred y se tiene que dar lugar a un cuello de botella.

4.- Capa de Transporte

La función de esta capa es aceptar todos los datos de la capa de sesión y a su vez dividirlos en unidades muy pequeñas para que pasen a la capa de red. También debe asegurar que estas unidades lleguen al otro extremo de la comunicación.

5.- Capa de Sesión

En esta capa se establecen las conexiones entre usuarios finales, a través de una sesión se puede permitir al usuario acceder al sistema.



En esta capa se proporcionan los siguientes servicios:

- Control de diálogo. Aquí la comunicación puede ser en dos sentidos o se puede ir alternando en los dos sentidos.
- Agrupamiento. De diferentes sistemas se puede agrupar la información para obtener un resultado final.
- Recuperación. Si hay alguna falla en el envío de información, la capa de sesión permite retransmitir todos los datos desde el punto de comprobación.

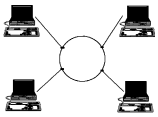
6.- Capa de Presentación

Esta capa se encarga de la presentación, es decir, de los aspectos de sintaxis y semántica de la información que se transmite, esto se debe a que hay distintos equipos que cuentan con diferentes formas de caracteres y la capa se encarga de mostrarlos de una manera entendible al usuario.

Además de contar con la función de formateo de datos (presentación), se tienen otras dos funciones importantes en esta capa que son el cifrado y la compresión de datos.

El cifrado se lleva a cabo para proteger la información que se trasmite, esto es, los datos no viajan en claro para que sólo sean entendidos por las personas autorizadas.

La compresión se lleva a cabo para reducir el tamaño de los datos que son transmitidos y funciona mediante el uso de algoritmos, en esta función todos los bits repetidos son reemplazados por un token (patrón de bit mucho más corto).



7.- Capa de Aplicación

Encargada de sincronizar las aplicaciones, además de controlar la integridad de los datos.

La función principal que se presenta en esta capa es la de dar servicio de correo electrónico, HTTP, FTP, SSH, FTP, TELNET.

Esta capa cuenta con funciones de implementación de aplicaciones distribuidas.