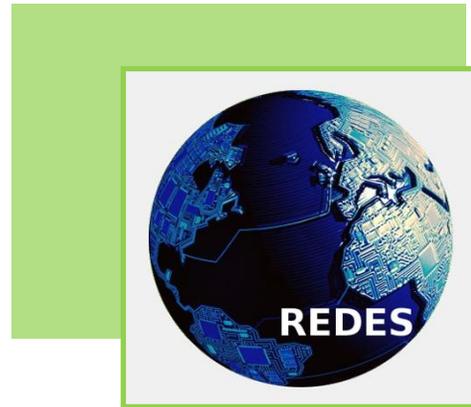


Capítulo 2

Conceptos de Redes

- 2.1 Contexto histórico de las redes**
- 2.2 Conceptos generales de redes**
- 2.3 Clasificación de redes**
 - 2.3.1 Redes LAN
 - 2.3.2 Redes MAN
 - 2.3.3 Redes WAN
- 2.4 Topologías de red**
 - 2.4.1 Estrella
 - 2.4.2 Anillo
 - 2.4.3 Bus
- 2.5 Medios de transmisión**
 - 2.5.1 Medios cableados
 - 2.5.2 Medios inalámbricos
- 2.6 Modelo de comunicación OSI**
 - 2.6.1 Capa física
 - 2.6.2 Capa de enlace de datos
 - 2.6.3 Capa de red
 - 2.6.4 Capa de transporte
 - 2.6.5 Capa de sesión
 - 2.6.6 Capa de presentación
 - 2.6.7 Capa de aplicación
- 2.7 Norma 802.3 de IEEE para redes de área local**
 - 2.7.1 Norma 802.3
 - 2.7.2 Direcciones Físicas
 - 2.7.3 Formato de las tramas físicas



En este capítulo se presentan los conceptos generales de las redes, sus topologías más comunes, los tipos que existen y una descripción del modelo de comunicación de Interconexión de Sistemas Abiertos, OSI (*Open System Interconnection*), que es un modelo de referencia para el diseño de protocolos de redes.

Una red se define como un conjunto de sistemas interconectados entre sí que comparten información y recursos entre ellos.

2.1 Contexto histórico de las redes

A principios del año 1968 el Departamento de Defensa de Estados Unidos aprobó y financió un proyecto que pretendía conectar universidades y otras instituciones con la finalidad de realizar investigaciones sobre nuevas tecnologías para compartir recursos e intercambiar información. Así fue como nació ARPANET (Red de la Agencia de Proyectos Avanzados de Investigación), la primera red de dispositivos, usada para la investigación y asuntos militares, con el propósito principal de descentralizar los servidores del Departamento de Defensa de Estados Unidos. Con esta red se realizó el primer envío de datos. Muy pronto se empezó a extender ARPANET y se fueron añadiendo más universidades a ella. La red funcionaba pero presentaba fallas frecuentemente y sus protocolos eran lentos. Tiempo después, entre 1980 y 1982, ARPANET adoptó el Protocolo de Control de Transmisión y el Protocolo de Internet (TCP/IP), que ya tenían varios años de haberse creado.

De forma separada al proyecto ARPANET, en 1972 en el Centro de investigaciones Xerox, en California, se comenzó a desarrollar un proyecto que pretendía conectar las computadoras de dicho centro de investigaciones y cualquier otra computadora que se quisiera. En 1973 este proyecto se denominó Ethernet y ya funcionaba dentro del centro de investigaciones con varias características que actualmente tiene la tecnología Ethernet¹.

Posteriormente ARPANET se dividió en dos partes, una seguía estando dedicada a la investigación, pero el Departamento de Defensa de Estados Unidos decidió crear otra red dedicada especialmente a los fines militares, ésta se llamó MILNET.

ARPANET continuó funcionando y se siguieron agregando redes a ella. Al unirse NSFNet (*National Science Foundation's Network*) fue que se empezó a utilizar el término Internet, para nombrar a cualquier red de área extensa que utilizara el protocolo TCP para la comunicación.

Para principios de los años 90 el correo electrónico ya no era novedad, pero estaba por iniciar un avance importante en las redes, la WWW (*World Wide Web*, amplia red mundial), una interfaz gráfica y con texto que pronto se convirtió en la preferida para enlazar a los usuarios a Internet. Fue entonces cuando surgieron los primeros navegadores, dada la creciente demanda del uso de hipertextos.

Durante varios años el medio utilizado para la comunicación de redes fue la línea telefónica, a pesar de no tener la capacidad que se requiere para transportar datos. Fue hasta finales de los años 90 y principios de la siguiente década cuando aparece la conexión de “banda ancha” y comienza a ser cada vez más utilizada para transferencia de datos, que para estos años ya no sólo era texto, sino imágenes, audio y video, lo cual requiere una alta velocidad en la transferencia.

En su inicio, las redes eran utilizadas por personas especializadas en el tema, pero con el tiempo el conocimiento requerido para poder usarlas se ha vuelto más intuitivo. Actualmente las redes ya forman parte de la vida cotidiana para muchas personas que deben usar dispositivos conectados entre sí, como cajeros automáticos, computadoras, cajas registradoras, verificadores de hora de entrada y salida, entre muchos otros.

2.2 Conceptos generales de redes

A cada uno de los sistemas que pertenecen a una red se le conoce como *nodo de red* y existen dos tipos: nodos terminales y nodos de conmutación. Un nodo terminal, o simplemente nodo, es el que genera y emite

¹ Llamado así en referencia a la teoría (errónea) de física que argumentaba que las ondas electromagnéticas viajaban a través de un fluido llamado éter.

datos (llamado emisor o remitente) y el que los recibe como destino final (conocido como receptor o nodo destino). Un nodo de conmutación es el que conecta diferentes redes. Los nodos se conectan entre ellos a través de un medio físico al cual se le conoce como *medio de transmisión* y puede ser por ejemplo un cable.

Los nodos son generalmente computadoras, pero puede ser cualquier dispositivo que forme parte de la red. Los términos equipo, dispositivo, *host* (en inglés) y máquina son formas de llamar a los nodos.

Se define como *red física* al conjunto de nodos interconectados directamente por hardware. Las redes físicas pueden estar basadas en diferentes tecnologías, por ejemplo Ethernet² y cada red física cumple una serie de normas establecidas para la tecnología de red con la que se diseña, incluyendo aspectos como la codificación empleada para representar los datos, la velocidad de transmisión, la forma de interconectar los nodos, entre otros.

En el nivel físico se especifican *direcciones físicas* que identifican de manera única a cada nodo dentro de la red. Para comunicar un nodo con otro se hace uso de sus direcciones físicas, también llamadas direcciones hardware y para el caso específico de Ethernet se llaman direcciones MAC.

En la tecnología Ethernet se especifica el uso de un nodo central al cual se conectan todos los demás, como se muestra en la Figura 2.1. Dicho nodo es un nodo de conmutación denominado concentrador (*hub*). Cada vez que un nodo tiene información que transmitir a otro envía el paquete al concentrador y éste decide por cual línea de salida reenviar la información. El concentrador necesita conocer las direcciones físicas de todos los dispositivos conectados a él ya que toma decisiones basadas en la dirección física que se indica en el paquete de datos.

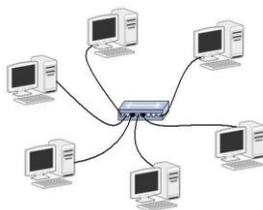


Figura 2.1 Red física con tecnología Ethernet

Una *red de redes* es un conjunto de redes físicas interconectadas en donde la tecnología de cada una es independiente de las demás. Se utiliza un software de bajo nivel que maneja la comunicación e interconexión del hardware y ofrece funciones a las capas de alto nivel en las que se ocultan los detalles de la implementación física de la red y permite que los nodos se comuniquen entre ellos sin importar a que red pertenecen, haciendo que parezca una sola red uniforme. Este diseño permite que los programas de aplicación sean independientes de la tecnología de red utilizada.

La red de redes permite enviar datos a través de redes intermedias sin necesidad de que los nodos origen y destino estén conectados directamente. Para que esto sea posible cada máquina debe poseer un identificador o dirección dentro de la red de redes para que cualquier equipo pueda acceder a ella. Esta dirección se denomina *dirección de red*, o *dirección lógica*, y es diferente de la dirección física, ya que especifica la ubicación de la red en donde reside el dispositivo.

Para interconectar redes se emplea un dispositivo llamado de forma general *compuerta de red*, y particularmente puede ser un *ruteador (router)* o una *puerta de enlace (Gateway)*. Una compuerta de red es un equipo que conecta redes físicas, de la misma manera que un concentrador conecta dispositivos. Así como el concentrador utiliza las direcciones físicas de los dispositivos conectados a él para saber a qué dispositivo encaminar los paquetes, la compuerta de red utiliza las direcciones de red para saber hacia qué red dirigir el tráfico. Un ruteador interconecta redes que utilicen un mismo protocolo en la capa de red, por ejemplo IP, y una puerta de enlace interconecta redes que utilizan diferentes protocolos.

² La tecnología Ethernet se explica con más detalle en el tema 2.8

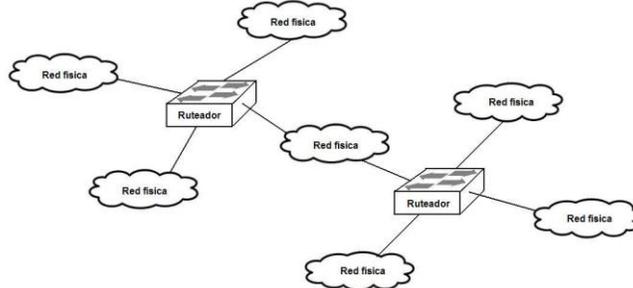


Figura 2.2 Diferentes redes físicas conectadas a través de routers

Las compuertas de red utilizan algoritmos de encaminamiento basados en las direcciones de red de los paquetes que requieren enviar. Los algoritmos de encaminamiento seleccionan la mejor ruta para cada paquete calculando el siguiente salto. Se llama “un salto” cada vez que el paquete atraviesa una compuerta de red para pasar de una red a otra, de tal manera que si un paquete que sale del nodo A dirigido hacia el nodo B pasa en su camino por dos compuertas de red, el paquete realizó dos saltos. La ruta de los paquetes desde el origen hasta el destino consiste en una sucesión de saltos. Cuando el paquete llega a la red final se utiliza el direccionamiento físico para saber a qué dispositivo de la red física tiene que ser entregado.

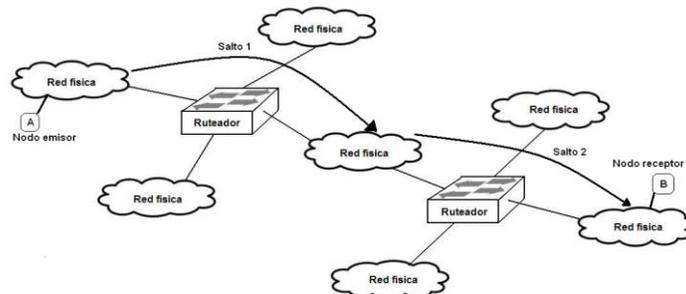


Figura 2.3 Sucesión de saltos de un paquete desde el nodo A hasta el nodo B

Una red de redes puede ser vista como una red virtual, en donde los dispositivos conectados a ella se comportan como si todos estuvieran en una gran red física conectados directamente unos a otros, sin importar lo que ocurra dentro de la red virtual. No es posible para dos dispositivos de diferentes redes comunicarse de manera directa, pero este aspecto es transparente para ellos. A la red de redes más grande que engloba a todas las redes existentes interconectadas se le denomina Internet.

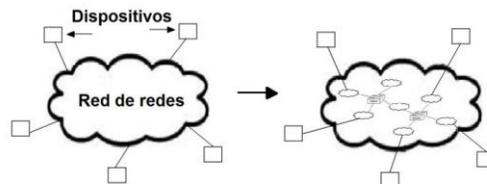


Figura 2.4 Red de redes vista como una sola red

2.3 Clasificación de redes

La extensión geográfica de la red y la manera en que se interconectan los nodos determina su clasificación en función de parámetros de velocidad y recursos a los que puede acceder de manera directa.

2.3.1 Redes LAN

Las Redes de Área Local, o LAN (*Local Area Network*), son aquellas que se distribuyen en un radio de 10 m a 1 Km aproximadamente, generalmente se localizan en pisos de algún edificio, en el edificio completo o en edificios adyacentes.

Características

- La velocidad de transmisión va desde 10 Mbps hasta 2000 Mbps³. Por ocupar un espacio menor que otro tipo de redes, la velocidad de transmisión es relativamente alta comparada con la velocidad de las redes MAN o WAN.
- Cada nodo de la red puede tener acceso a archivos, aplicaciones y recursos de hardware conectados a la red.
- Los nodos pueden comunicarse entre ellos sin necesidad de acceso a una red más grande como Internet.
- Los retardos pueden llegar hasta los 10 ms⁴.

2.3.2 Redes MAN

Las Redes de área Metropolitana, o MAN (*Metropolitan Area Network*), son las que ocupan un radio entre 1 y 100 km aproximadamente. Pueden ocupar partes de una ciudad o ciudades completas. Generalmente son redes tipo LAN interconectadas pero por su extensión no pueden ser consideradas una red LAN o WAN. El caso particular de las conexiones ADSL, usada por la mayoría de las personas con acceso a internet desde casa, entra en la clasificación de redes MAN ya que la conexión se puede realizar siempre y cuando el cableado que va del cliente a la central no exceda los 5 Km.

Características

- Para conectar varias redes LAN y formar una red MAN se requieren nodos de conmutación.
- La velocidad de transferencia es mayor que la de una red WAN pero menor a la de una red LAN, debido a que los nodos de conmutación agregan un retardo a los datos enviados.

2.3.3 Redes WAN

Las Redes de Área Extensa, o WAN (*Wide Area Network*), son aquellas que se distribuyen en distancias mayores a 100 Km. Pueden abarcar hasta continentes enteros.

Características

- Las velocidades de transferencia de datos van desde los 56 kbps hasta los 155 Mbps⁵.
- Las redes de área extensa necesitan diferentes tipos de nodos de conmutación para comunicar nodos que pueden pertenecer a diferentes tipos de redes.

2.4 Topologías de red

La topología (del griego *topos*=lugar y *logos*=estudio) es la forma de conectar los nodos dentro de una red. La topología es relevante ya que la velocidad de transmisión y la cantidad de cable utilizado para las conexiones afectan de diferente forma el rendimiento de la red según se elija una topología u otra. Esto hace que cada topología tenga ventajas y desventajas frente a las demás. Las topologías utilizadas en redes se presentan a continuación.

2.4.1. Estrella

Esta topología consiste en conectar todos los nodos a un nodo principal, de tal forma que el nodo principal funcione como un intermediario para los demás. Esta topología es utilizada generalmente en redes locales y el nodo principal puede ser un ruteador, un conmutador o un concentrador.

³ COMER, DOUGLAS E. *Redes globales de información con Internet y TCP/IP Vol.1; Principios básicos, protocolos y arquitectura*, 3ª edición: Prentice-Hall, 1996. Página 19.

⁴ COMER, DOUGLAS E. *Obra citada*, 1996. Página 19.

⁵ COMER, DOUGLAS E. *obra citada*, 1996. Página 19.

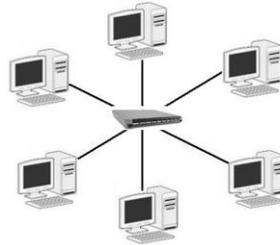


Figura 2.5 Topología en estrella

Ventajas

- Todos los nodos pueden enviar información y recibirla sin que tenga que pasar por los demás nodos.
- Sin un nodo falla el funcionamiento de la red no se ve afectado.
- No se necesitan conectores especiales para introducir equipos nuevos a la red.
- La implementación es sencilla.

Desventajas

- Si el nodo principal falla la red deja de funcionar por completo.
- Requiere mayor cantidad de cable comparada con la topología en anillo o en bus.

2.4.2. Anillo

Esta topología consiste en conectar cada nodo de la red con el siguiente nodo, y el siguiente con el que le sigue y así sucesivamente hasta que el último nodo se conecte al primero. En esta topología los datos sólo viajan en una dirección, por lo que al enviar información, por ejemplo, del primer nodo al último, la información debe pasar por todos los nodos, no así si el último requiere enviar información al primero, ya que esa conexión es directa. Debido a esto existe también la topología en anillo doble, lo que permite conectar a un grupo de nodos de la misma forma pero el envío de datos puede ir en ambos sentidos.

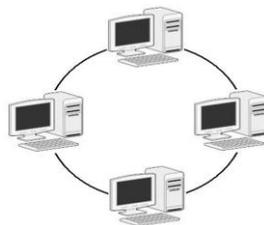


Figura 2.6 Topología en anillo

Ventajas

- Su implementación es sencilla.
- El cableado es menor al requerido en otras topologías.

Desventajas

- Si un nodo de la red falla, la comunicación en toda la red se pierde.
- Los datos, generalmente, deben pasar por muchos nodos antes de llegar a su destino.

2.4.3. Bus

Esta topología consiste en un solo canal de comunicación que comparten todos los nodos de la red, para poder comunicarse se deben establecer permisos para ocupar el medio ya que las colisiones se presentan con frecuencia.

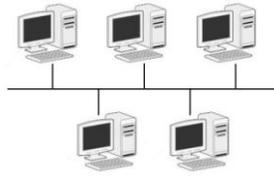


Figura 2.7 Topología en bus

Ventajas

- El cableado es considerablemente menor que el de la topología en estrella.

Desventajas

- El medio debe estar correctamente terminado en los extremos del bus, si no la red puede tener fallos.
- Las colisiones son constantes y provocan problemas en la red, se requieren métodos para evitarlos.
- Se requieren conectores especiales para agregar nuevos nodos a la red.

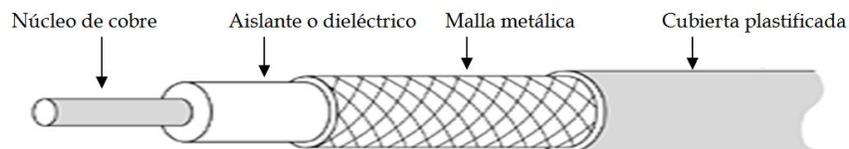
2.5 Medios de transmisión

El medio por el que son transportados los datos determina cuestiones como la velocidad de transmisión (en bps, bits por segundo), el nivel de interferencia u otros ruidos⁶ que pueden sufrir las señales con los datos. Este medio puede ser cableado o inalámbrico.

2.5.1 Medios cableados

Los medios de transmisión cableados son aquellos que utilizan algún tipo de cable para transportar los datos. Estos cables por lo general están hechos de cobre cubiertos por algún aislante y con recubrimiento plastificado. Existen varios tipos de medios cableados. A continuación se presentan los que se utilizan para cableado en redes de computadoras.

Cable coaxial. Es un cable compuesto por un núcleo conductor (cobre generalmente) con un aislante o dieléctrico, el cual es cubierto a su vez por una malla delgada de metal conductor (cobre generalmente) y un capa aislante plastificada. En la Figura 2.8 **Error! No se encuentra el origen de la referencia.** se indican las secciones que conforman un cable coaxial.

Figura 2.8 Secciones de un cable coaxial⁷

El núcleo del cable es el que lleva los datos; el aislante o dieléctrico separa el núcleo de la malla metálica, esta malla es la referencia a tierra. La cubierta plastificada sirve para aislar todo el cable y protegerlo de la intemperie. El cable puede estar apantallado o no, el apantallamiento consiste en una capa de algún material (generalmente aluminio) entre la malla metálica y el dieléctrico y se usa para evitar ruido en la señal.

Cable de pares trenzados. Este tipo de cable consiste en determinado número de pares de cables de cobre de 1mm de espesor generalmente, aislados con un recubrimiento plástico, torcidos en pares y envueltos en un

⁶ El ruido es cualquier perturbación que modifique de forma indeseada la señal que se transmite. La interferencia es la señal que se produce cuando una señal altera la integridad de otra. La interferencia es un caso particular del ruido, ya que es una perturbación provocada generalmente por la superposición de la señal deseada y alguna otra señal no deseada.

⁷ Tanenbaum, Andrew S. *Redes de computadoras*. 4ª edición: Prentice Hall. 2003. Página 74.

recubrimiento plástico que contiene a todos los pares del cable. El propósito de trenzar los pares de cables es aislar los hilos de la interferencia eléctrica y magnética que se provoca por los pares cercanos a cada par y por otros dispositivos externos. En la Figura 2.9 se presenta un cable de cuatro pares trenzados.

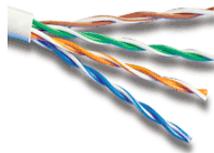


Figura 2.9 Cable de 4 pares trenzados

Cada hilo en un cable de par trenzado tiene un color diferente, estos colores están estandarizados para una fácil identificación y armado del cableado de una red. Los colores para este tipo de cable con cuatro pares de hilos son:

- Blanco–Azul
- Azul
- Blanco–Verde
- Verde
- Blanco–Marrón
- Marrón
- Blanco–Naranja
- Naranja

El cable de pares trenzados puede ser blindado (*Shielded Twisted Pair*, STP) o sin blindar (*Unshielded Twisted Pair*, UTP). El primero tiene una malla metálica que recubre los pares trenzados mientras que el segundo carece de ella. El blindaje es primordialmente para evitar ruido en las señales que viajan por los pares trenzados, el más usado es el UTP.

Existen diferentes categorías de cable, cada una con características eléctricas propias que los hacen adecuados para diferentes aplicaciones.

- **Categoría 1.** Hace referencia al cable telefónico tradicional que resulta adecuado para transmitir voz, pero no datos. La mayoría de los cables telefónicos instalados antes de 1983 eran cables de Categoría 1.
- **Categoría 2.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 4 Mbps. Este cable consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 3.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 10 Mbps aproximadamente. Consta de cuatro pares trenzados de hilo de cobre con tres entrelazados por pie.
- **Categoría 4.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 16 Mbps aproximadamente. Consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 5.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 100 Mbps aproximadamente. Consta de cuatro pares trenzados de hilo de cobre.

Para armar el cableado de una red con cable de pares trenzados se tienen dos configuraciones con propósitos particulares, cada una estandarizada en una norma que asigna un color diferente a cada terminal del conector RJ45, la norma 568A y la 568B. En la Figura 2.10 se muestra la configuración especificada por cada una de las normas.

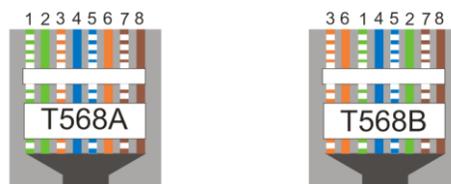


Figura 2.10 Normas para la configuración de cables de pares trenzados

Fibra óptica. Consiste en un hilo delgado, llamado núcleo, de fibra de vidrio o algún material plástico recubierto con un aislante. Por este núcleo pasan rayos de luz hasta llegar al otro extremo haciendo uso de la propiedad de reflexión. Este medio alcanza velocidades de transmisión de hasta 1000 Mbps y es muy utilizado en telecomunicaciones debido a que es prácticamente inmune a interferencias y la atenuación que sufren las señales transmitidas es muy baja. Existen dos tipos de fibra óptica:

Multimodo. El núcleo tiene un diámetro de 200 micrómetros, lo cual hace que la luz pueda tomar diferentes caminos hasta llegar al otro extremo de la fibra.

Ventajas

- Es más económico que la fibra monomodo.
- Es más fácil de conectar que la fibra monomodo ya que el diámetro del núcleo es mucho mayor y se pueden usar materiales de menor precisión para las conexiones.

Desventajas

- Solo se pueden utilizar en distancias menores a 1 Km.

Monomodo. El núcleo tiene un diámetro entre 8 y 10 micrómetros, lo cual hace que la luz sólo pueda seguir un solo camino hasta el otro extremo de la fibra.

Ventajas

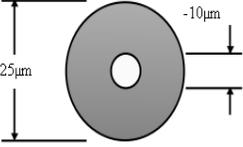
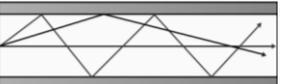
- Su velocidad de transmisión se encuentra en el orden de decenas de Gbps.
- Se puede usar en largas distancias, 300 Km como máximo.

Desventajas

- Entre menor sea el diámetro del núcleo la fibra y los materiales para las conexiones serán más costosos.

En la Tabla 2-1 se presenta un bosquejo del diámetro de los dos tipos de fibra y un esquema del modo de propagación que utiliza cada uno.

Tabla 2-1 Sección transversal y esquema de modo de propagación de los tipos de fibras ópticas

	Fibra multimodo	Fibra monomodo
Diámetro		
Esquema del modo de propagación		

2.6.2 Medios inalámbricos

Los medios inalámbricos son aquellos que no son guiados mediante un cable y refieren al aire o el vacío, ya que es a través de éstos por donde se propagan las señales. Debido a esto se hace necesario el uso de antenas para la transmisión y recepción de las señales. Las microondas, las señales de radio, TV comercial, infrarrojo y *bluetooth* son algunos ejemplos de señales que viajan por un medio inalámbrico.

2.6 Modelo de comunicación OSI

Para estudiar los sistemas de comunicaciones de redes, se emplea un modelo conceptual en el que el trabajo de transportar información de un lugar a otro se divide en niveles, llamados comúnmente capas, donde cada una tiene una tarea específica dentro de la comunicación.

El modelo OSI (Interconexión de Sistemas Abiertos) es un modelo conceptual creado por la ISO (*International Organization for Standardization*) que sirve como referencia cuando se requiere realizar la implementación de una pila de protocolos. Los protocolos son especificaciones y reglas que indican el procedimiento que se debe seguir en cada etapa de la comunicación, sirven para que dos equipos que se comunican a través de una red puedan entenderse e interpretar de manera correcta la información que comparten.

El modelo OSI se divide en siete niveles o capas. Cada capa de un nodo emisor se comunica virtualmente con la misma capa del nodo destino y físicamente con la capa inferior y la capa superior. En la Figura 2.11 se presenta un diagrama del modelo OSI. Las líneas punteadas indican la comunicación virtual entre las mismas capas de ambos nodos y las líneas sólidas la comunicación física dentro de un mismo nodo.

Cuando una capa le entrega datos a otra de un nivel inferior se dice que el nivel inferior *encapsula* los datos, agregándole sus encabezados.

Un encabezado es un conjunto de bits que un protocolo añade a la información. Cada protocolo define cierto número de bits, especifica su contenido y formato, así como la acción que se debe realizar dependiendo del valor de los bits del encabezado.

El flujo de los datos inicia en la capa de aplicación cuando existe información para enviar a otra aplicación en un equipo remoto. Los datos se pasan de la capa de aplicación a la de presentación, donde se añaden los encabezados de esta capa, pasando posteriormente a la de sesión, agregando los encabezados correspondientes y así sucesivamente con el resto de las capas hasta llegar a la capa física donde los datos son convertidos en señales que finalmente se transmiten por el medio físico.

En el lado receptor se ejecuta el proceso inverso, las señales son recibidas por el medio físico, donde se convierten en datos y se pasan a la capa de enlace. La capa de enlace verifica el contenido del encabezado correspondiente para realizar sus funciones, posteriormente pasa los datos a la capa de red y así sucesivamente hasta ser entregados a la aplicación correspondiente.

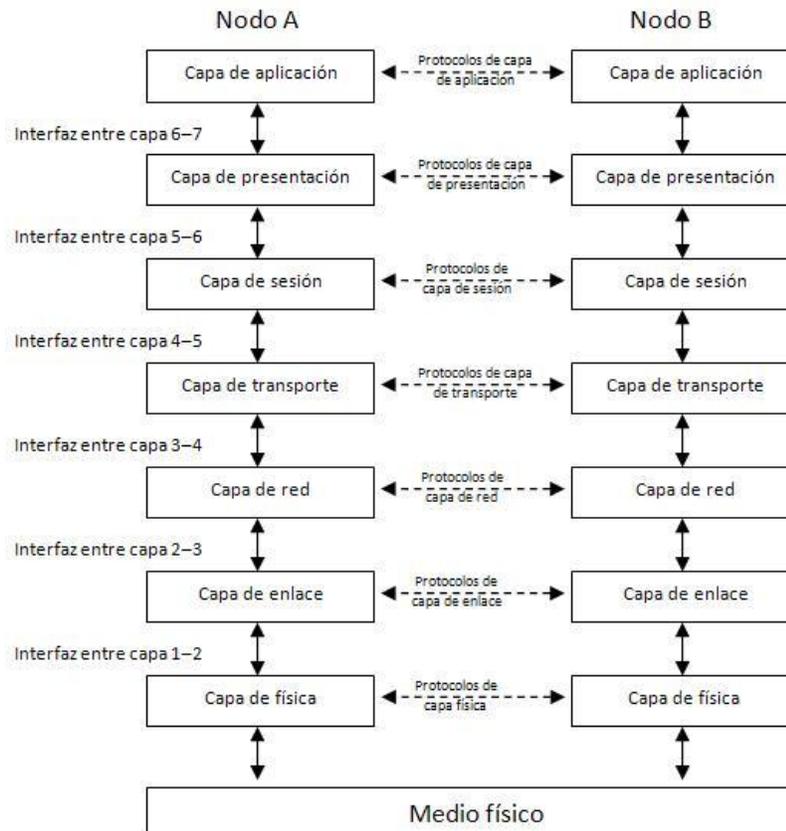


Figura 2.11 Diagrama con la división de capas del modelo OSI⁸

A continuación se presenta un ejemplo para explicar el funcionamiento del modelo de referencia OSI, haciendo una analogía con mensajes escritos en papel y enviados con un mensajero.

Ejemplo. Modelo de comunicación Empresario-Secretaria-Mensajero⁹.

Este modelo está dividido en varios niveles, cada uno realiza actividades específicas y bien definidas que son indispensables para que los mensajes lleguen a su destino.

En cierta ciudad hay dos edificios separados por varias calles, uno pertenece a la empresa A y el otro a la empresa B, encabezadas por sus respectivos directivos: el empresario A y el empresario B; los cuales hablan idiomas diferentes y solamente su idioma. Cada empresario tiene una secretaria, que habla el idioma de su jefe y además otro que ambas conocen. El asunto importante es que los empresarios deben comunicarse constantemente ya que cada empresa depende de la otra.

Analizando el flujo de los datos:

En el edificio que emite el mensaje.

El empresario A escribe el mensaje que requiere enviar al empresario B y llama a su secretaria para entregárselo.

La secretaria recibe el mensaje y lo traduce al idioma que ella y la otra secretaria conocen. Luego de hacer la traducción le pone el sello de la empresa, lo coloca dentro de un sobre y escribe el nombre de la

⁸ Tanenbaum, Andrew S. *obra citada*. Página 37.

⁹ Basado en el ejemplo presentado en Tanenbaum, Andrew S. *obra citada*. Páginas 29 y 30.

secretaria a la cual va dirigido, el nombre de la secretaria que lo envía y la hora de salida. Entonces, llama al mensajero y le entrega el sobre.

La actividad del mensajero consiste en colocar el sobre en su mochila y recorrer el trayecto en bicicleta hasta el edificio B. Al llegar saluda al mensajero que se encuentra en la entrada y le entrega el mensaje.

En el edificio que recibe el mensaje.

El mensajero recibe el sobre, revisa el nombre de la secretaria a la que va dirigido y se lo entrega en persona.

La secretaria revisa que su nombre esté escrito en el sobre, lo abre para leer el contenido y poder traducirlo en el idioma que su jefe entiende. Una vez traducido, va a la oficina de su jefe y le entrega el mensaje.

El empresario recibe la traducción del mensaje y comienza a leerlo.

Es importante notar que los mensajeros tienen comunicación entre sí, al igual que las dos secretarias y los empresarios (lo cual es el objetivo) aunque el flujo de los datos realmente sea Empresario–Secretaria–Mensajero del lado emisor y Mensajero–Secretaria–Empresario en el lado receptor.

En la Figura 2.12 se presenta un diagrama con las capas que conforman este modelo de comunicación.

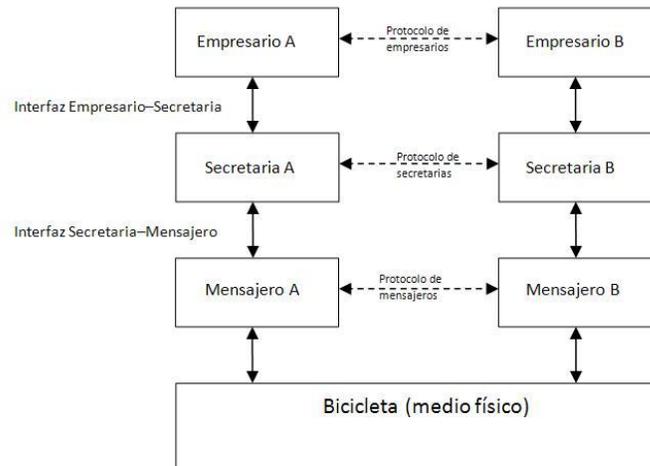


Figura 2.12 Diagrama con la división en capas del modelo de comunicación Empresario-Secretaria-Mensajero

A continuación se describe la función de las capas del modelo OSI.

2.6.1 Capa física

La capa física determina cuestiones tales como el medio físico por donde se transmite la información, la codificación que se emplea, los niveles de voltaje, la forma en que se interconectan los dispositivos de la red y los tipos de conectores necesarios, entre otras. En este nivel la unidad de datos son los bits.

2.6.1.1 Conmutación

La conmutación es una parte importante en una red ya que los conmutadores encaminan los datos para que lleguen a su destino. Los métodos de conmutación más comunes son los siguientes.

Conmutación de circuitos. En la conmutación de circuitos el nodo que requiere enviar datos debe tener una ruta previamente establecida entre el nodo receptor y el nodo emisor. Esto se ve más claramente en la línea telefónica, ya que para establecer una comunicación, al marcar el número se busca el camino que deben seguir los datos y una vez definido se entabla la comunicación.

Conmutación de paquetes. Consiste en enviar paquetes, que contienen datos o información de control, a centrales de conmutación. En cada paquete se especifica el destino de modo que la central de conmutación sepa a dónde dirigirlo. En la Figura 2.13 a) se muestra cómo se realiza la conmutación de circuitos y en la Figura 2.13 b) la conmutación de paquetes de datos.

Los IMP (*Interface Message Processor*) fueron los primeros circuitos que realizaban la conmutación de paquetes en redes como ARPANET. Los nodos de conmutación funcionan como las centrales de conmutación de paquetes y es común en la literatura de redes encontrar el término *central de conmutación* o *IMP* como sinónimo de nodo de conmutación.

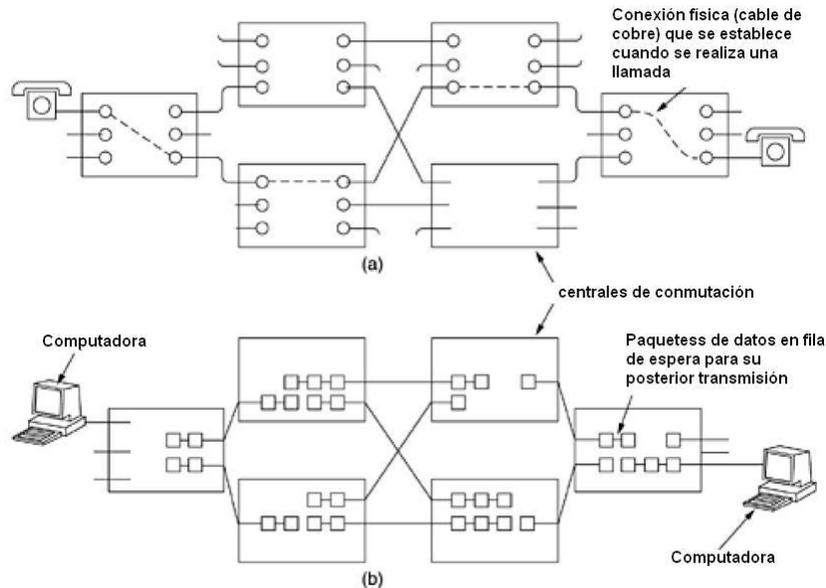


Figura 2.13 a) Conmutación de circuitos. b) Conmutación de paquetes de datos¹⁰

2.6.1.2 Códigos de línea

Otro punto importante que se trata en la capa física refiere a la codificación de los datos, es decir, la conversión de datos en señales para poder ser transmitidos por un medio físico y viceversa.

Se llama código de línea al código aplicado a los datos con el propósito de que sean transmitidos físicamente. Se han desarrollado diferentes tipos de códigos de línea para codificar datos de tal forma que el receptor pueda identificar qué valor debe tener un determinado bit en una señal.

Los bits se representan con niveles de voltaje, generalmente un nivel de voltaje alto representa un uno lógico y un nivel bajo representa un cero lógico, pero las representaciones pueden variar, además es necesario que los datos estén sincronizados con un reloj para determinar dónde empieza y dónde termina un bit y poder leer todos los bits de una señal. Existen tres tipos de codificación:

- No retorno a Cero, o NRZ (*Non Return to Zero*). Cada bit mantiene el mismo valor durante todo el ciclo de reloj, ya sea el nivel alto o bajo de voltaje.
- Retorno a Cero, o RZ (*Return to Zero*). Cada bit ocupa la mitad del ciclo de reloj para representar su valor y la otra mitad del ciclo su valor es cero volts.
- Codificación Bifase. Los bits presentan una transición entre voltaje alto y voltaje bajo a la mitad del ciclo de reloj que indica de qué valor lógico se trata.

Cada tipo de codificación utiliza métodos particulares, por ejemplo, la tecnología Ethernet utiliza un método denominado *Manchester*, el cual es un tipo de codificación bifase. Con este método el receptor se puede sincronizar usando la señal que contiene los datos al tomar de ella los tiempos de bit, es decir, la

¹⁰ Tanenbaum, Andrew S. *obra citada*, página 113.

señal de reloj está incluida dentro de la misma señal de datos (ver Figura 2.14). Aun cuando la codificación Manchester ocupa el doble de ancho de banda que una codificación NRZ, la sincronía es la que permite desechar muchas veces otros métodos para codificar datos.

En la codificación Manchester siempre hay una transición en la mitad del intervalo de tiempo de bit. Se toman los cambios de la señal alto–bajo y bajo–alto como la representación lógica de un cero o un uno respectivamente. El receptor puede sincronizarse con el transmisor usando las transiciones en la señal de datos como señal de reloj.

Si se presentan bits adyacentes con el mismo valor, se produce una transición en el inicio del segundo bit, la cual no es tomada en cuenta por el receptor al momento de decodificar, sólo las transiciones separadas uniformemente en el tiempo son las que se consideran.

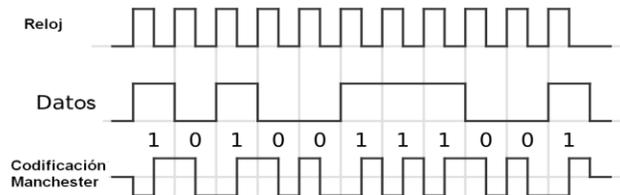


Figura 2.14 Codificación Manchester

2.6.2 Capa de enlace de datos

El propósito de este nivel es asegurar la entrega de paquetes entre dos equipos conectados directamente (equipos que pertenecen a una misma red física). Garantiza que la capa de red del receptor reciba datos libres de error, fragmenta la información si es necesario, controla el correcto acceso al medio y verifica que los paquetes que se han entregado a un destino correspondan a los que se enviaron desde el origen y que estén en el mismo orden. La unidad de datos que maneja este nivel se denomina trama. Para crear y reconocer tramas, el nivel de enlace delimita su inicio y su fin, además de detectar si fueron recibidas correctamente o no. En general la capa de enlace ofrece cuatro servicios a la capa de red:

- Transferencia de datos
- Control de errores
- Control de Flujo
- Creación de tramas

La capa de enlace se divide en la subcapa de Control de Acceso al medio, o MAC (*Medium Access Control*), que se encuentra ubicada sobre la capa física e interactúa directamente con ella, y la subcapa de Control de Enlace Lógico, o LLC (*Logical Link Control*), ubicada debajo de la capa de red.

2.6.2.1 Subcapa de Control de Acceso al Medio.

Cuando la red comparte el medio de transmisión entre todos sus dispositivos, la capa de enlace establece mecanismos que determinan quien tiene derecho a usar el medio para transmitir. A estos mecanismos se les llama métodos de contienda por el acceso al medio.

Para asignar el acceso al medio se han diseñado protocolos que permiten evitar colisiones entre paquetes cuando varios nodos requieren enviar datos por el mismo medio. Se denominan protocolos CSMA (*Carrier Sense Multiple Access*, Protocolos de Múltiple Acceso al Medio por Detección de Portadora) a los protocolos en los que los nodos que envían datos monitorean el estado del medio de transmisión para determinar en qué momento éste se encuentra libre y es posible enviar información. Hay varios tipos de protocolos CSMA, pero el más utilizado es el que implementa la detección de colisiones (CD, Collision Detect), denominado CSMA/CD.

El protocolo CSMA/CD tiene ventajas sobre otros protocolos, debido a que además de verificar si el medio de transmisión está desocupado, le brinda a todos los nodos el mismo derecho de usarlo. Si dos o más nodos envían datos al mismo tiempo se presenta una colisión y los nodos involucrados detienen inmediatamente la transmisión, esperan un intervalo de tiempo aleatorio y vuelven a ejecutar el algoritmo.

2.6.2.2 Subcapa de Control de Enlace Lógico.

La Subcapa de Control de Enlace Lógico provee los mecanismos de control de flujo y multiplexión para hacer posible la comunicación por un mismo medio. Esta subcapa genera tramas a partir de los datos provenientes de la capa de red, recibe las tramas que envían otros equipos y pasa la información a la capa de red. También se ocupa de la detección y corrección de errores.

La comunicación entre la capa de enlace y la capa de red se realiza utilizando algunas formas básicas de comunicación entre las capas, llamadas primitivas de servicio: solicitud, indicación, respuesta y confirmación.

2.6.2.3 Control de error e integridad de los datos

Los errores pueden presentarse por diversos motivos, tales como interferencia, mal estado del medio de transmisión y ruido eléctrico, por mencionar algunos, lo cual provoca que los datos no lleguen o lleguen alterados a su destino.

Cuando los bits llegan a un nodo son recibidos por la capa física, de donde pasan a la capa de enlace, pero no se garantiza que estén libres de errores. La cantidad de bits recibida puede ser diferente de la que se debe recibir y es responsabilidad de la capa de enlace detectar y corregir los errores que se presenten. Para tal efecto la capa de enlace del emisor crea un código de redundancia que es insertado en los datos y que al ser recibidos la capa de enlace del receptor verifica para comprobar su integridad. El código de redundancia es una cantidad que se calcula a partir del contenido de los datos, por lo tanto si algún dato se altera o se pierde, al volver a calcular el código éste será diferente.

2.6.2.4 Control de flujo.

Un aspecto importante que la capa de enlace debe gestionar se presenta cuando un emisor envía datos a una velocidad mayor a la que un nodo destino puede recibirlos. Si no se tiene control sobre esta situación, aun cuando el receptor no indique que existe un error, los datos podrían perderse, debido a que en algún momento dado el receptor no tendría espacio suficiente para almacenarlos y los desecharía. Introduciendo el control de flujo el receptor puede indicarle al emisor la cantidad de datos que puede recibir. Si se llena la memoria de recepción el receptor puede indicar al emisor que detenga su envío. Después de procesar los datos y liberar espacio en la memoria, le indica al transmisor que está listo para recibir más datos. Esta indicación se realiza mediante *tramas de pausa*. Al recibir esta trama el emisor deja de transmitir, espera a que concluya el tiempo solicitado y después reanuda su transmisión.

2.6.2.5 Protocolos de enlace

Para el envío y recepción de tramas se requieren métodos que reciban los datos de la capa superior, generen y envíen tramas. Los protocolos de enlace son los que realizan estas tareas y los más utilizados son los de ventana deslizante. Este tipo de protocolos utilizan un mecanismo para el control de flujo de datos en forma bidireccional entre emisor y receptor. El algoritmo de estos métodos no sólo se aplica en la capa de enlace sino en la capa de red o en cualquier otra capa que pudiera requerir un funcionamiento similar.

Cada emisor puede enviar cierta cantidad de datos y cada receptor puede recibirlos ya sea en menor, igual o mayor cantidad. La función de la ventana deslizante es evitar que el receptor se sature de datos y sólo permita la llegada de los que puede procesar.

Cada extremo de la conexión mantiene un buffer (memoria temporal de almacenamiento) de transmisión con una ventana de transmisión y un buffer de recepción con una ventana de recepción. El emisor transmite una cantidad de tramas definida por el tamaño de la ventana, y el buffer espera recibir la confirmación de cada una, sin poder enviar más datos hasta que esto ocurra. Al mismo tiempo que se envía una trama se pone en operación un contador para evitar que el emisor se quede esperando la confirmación de tramas que se pierden en el camino, y si el contador llega a un determinado valor sin haber recibido aún la confirmación, entonces el paquete se reenvía, asumiendo que no llegó a su destino. Una vez confirmada una trama, los datos salen de la ventana y ésta se recorre para enviar y esperar la confirmación de los datos que aún no se han transmitido, pero los que quedan fuera de la ventana siguen en espera.

En la Figura 2.15 se ilustra el concepto de ventana deslizante. En el inciso a) se representa un buffer de transmisión. Tomando a los números del buffer como paquetes, el tamaño de la ventana es una cantidad de bytes tal que abarca diez paquetes, que se envían a su destino. En el inciso b) se supone que el extremo receptor envió la confirmación de tres paquetes, entonces la ventana se recorre tres lugares, dejando fuera los datos que ya han sido confirmados y agregando nuevos datos que procede a enviar inmediatamente. Los datos que quedan a la izquierda de la ventana pueden borrarse y los que quedan a la derecha siguen esperando para ser enviados. Cuando el buffer se llena por la parte derecha, almacena más información en el espacio de la izquierda, pensando en el buffer como si fuera cíclico.

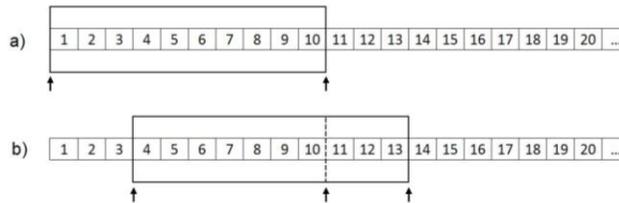


Figura 2.15 Ventana con 10 espacios de almacenamiento. a) Comienza en el espacio 1 y llega al 10, estas tramas ya se han enviado y esperan la confirmación de recepción. b) Una vez confirmadas 3 de las tramas enviadas la ventana deslizante avanza 3 lugares

La ventana en el lado del receptor indica al emisor el espacio de memoria que tiene disponible, esto es, la cantidad de bytes con que cuenta para almacenar datos que espera recibir, debe ser menor o igual al espacio libre en su buffer de recepción. Si no se conoce el espacio de almacenamiento de un dispositivo, un emisor puede exceder ese tamaño y saturar al receptor.

2.6.3 Capa de red

La capa de red es la encargada de proporcionar la conectividad necesaria para que dos nodos distantes puedan tener comunicación entre ellos, selecciona la ruta por la que se enviarán los datos, se apoya en los servicios que le proporciona la capa de enlace y a su vez brinda servicio a la capa de transporte. Los datos que se manejan en la capa de red reciben el nombre de paquetes.

2.6.3.1 Tipos de servicio

La capa de red puede funcionar de dos formas diferentes: estableciendo una conexión lógica o sin establecerla. Dependiendo de estas formas de funcionamiento esta capa proporciona diferentes tipos de servicios.

Si se establece una conexión se le conoce como *circuito virtual*, haciendo alusión a la forma en que se conmutan los circuitos en las centrales telefónicas para realizar una llamada (estableciendo la conexión antes de iniciar el envío de mensajes). Si no se utiliza una conexión, entonces el envío de paquetes será independiente y cada uno deberá incluir el destinatario dentro de un encabezado, a estos paquetes se le conoce como *datagramas*, en analogía con los telegramas del servicio postal, ya que su funcionamiento es similar.

Los circuitos virtuales se utilizan en subredes cuyo servicio principal está orientado a la conexión, lo cual evita decidir el camino que tomará cada paquete. Una característica al establecer una conexión y hacer uso de los circuitos virtuales es que cada paquete de datos enviados no contenga el encabezado de dirección destino, sino únicamente el primero, dado que los que se transmiten después ya tienen un camino marcado para llegar a su destino.

Contrario a los circuitos virtuales, en una red que maneja datagramas, ninguna ruta se puede establecer previamente porque cada paquete se envía de forma independiente y cada uno puede seguir diferentes rutas. Dependiendo de la ruta que tomen los datos, un datagrama puede llegar antes o después que otro, es decir, los datagramas no llegan necesariamente en el mismo orden en que fueron enviados.

2.6.3.2 Encaminamiento

Parte del trabajo de la capa de red es encontrar el camino que deben seguir los datos y éste debe elegirse dependiendo de la congestión de la red, las longitudes de la cola de espera en los nodos de conmutación, retardo y velocidad del medio. Los encargados de realizar esta tarea en el nivel de red son los ruteadores

(*routers*), los cuales se encargan de buscar el mejor camino por el que se puedan enviar los datos. Existen dos tipos de algoritmos de encaminamiento utilizados por los ruteadores, los adaptativos y los no adaptativos.

Los algoritmos no adaptativos no basan sus decisiones en mediciones o estimaciones del tráfico de la red o su topología, sino que la ruta a seguir se determina anticipadamente al poner en funcionamiento a la red.

Los algoritmos adaptativos utilizan información sobre el estado de la red y toman la decisión de seguir una u otra ruta dependiendo de dicha información.

2.6.3.3 Manejo de errores

Cuando se genera un error en la entrega de un paquete que atraviesa varias redes a través de distintos ruteadores, el ruteador que detecta el error puede informar al nodo origen sobre lo ocurrido. Por ejemplo supongamos que un ruteador contiene información incorrecta u obsoleta, lo cual provoca que direcciona un datagrama hacia un ruteador incorrecto, que no encontrará un camino para reexpedir el paquete hacia el destino adecuado. En un caso como este, el último ruteador no sabrá qué hacer con el paquete y, como no sabe de qué punto anterior proviene, no lo puede regresar para que sea guiado por un camino adecuado, así que lo desecha. La única información que el ruteador conoce sobre el paquete es la dirección del nodo en donde fue originado. Esto le permite generar un reporte sobre lo ocurrido y notificar al nodo emisor. Las medidas de corrección que se puedan tomar para errores en la entrega de paquetes las realiza el emisor basado en la información del error ocurrido.

2.6.3.4 Congestión y Bloqueos

Otro tema importante que se debe tratar en la capa de red es la congestión. Los ruteadores reciben paquetes de otros ruteadores o del emisor directamente para que sean enviados a sus destinos; esta función la realizan sin dificultad mientras operan dentro de los límites de sus capacidades de procesamiento y memoria. La congestión se presenta cuando las filas de espera en las centrales de conmutación se hacen muy largas debido a que dichas centrales no tienen la capacidad suficiente para procesar tantos paquetes de datos al mismo tiempo. Este inconveniente se presenta comúnmente en las subredes o parte de ellas.

El bloqueo es el peor de los escenarios de una congestión, ya que en esta situación los paquetes ya no entran ni salen de un ruteador. No pueden entrar debido a que la central llega a su capacidad máxima de almacenamiento y no pueden salir porque otras centrales presentan la misma situación. El algoritmo de Schweitzer y el de Blazewicz son los más utilizados para resolver el problema del bloqueo.

2.6.3.5 Interconexión de redes

Para tener comunicada a una red con otra u otras más es necesario saber qué tipo de redes se conectan, ya que redes LAN o WAN pueden necesitar comunicarse pero en realidad no son compatibles entre sí.

Para hacer fluir datos entre redes diferentes se utilizan los llamados *retransmisores*, los cuales son específicos para cada conexión. Los diferentes tipos de retransmisores se enlistan a continuación.

Repetidores. Copian los bits individualmente entre segmentos de cable, actúan en la capa física.

Puentes (*bridges*). Almacenan y reexpiden tramas entre redes LAN, actúan en la capa de enlace.

Puertas de enlace (*Gateway*). Almacenan y reexpiden paquetes entre redes que no son similares, actúan en la capa de red.

Particularmente las puertas de enlace y los puentes son nodos de conmutación que permiten comunicar unas redes con otras.

2.6.4. Capa de transporte

La tarea de esta capa es llevar los datos de forma segura y económica hasta el nodo destino, sin depender de la red o redes físicas que se encuentren en uso. La unidad de datos que utiliza recibe el nombre de TPDU (*Transport Protocol Data Unit*) Unidad de Datos del Protocolo de Transporte. En algunos protocolos particulares de la capa de transporte los datos reciben el nombre de segmentos o datagramas.

2.6.4.1 Servicios proporcionados a la capa de sesión

De forma similar a la capa de red, la capa de transporte proporciona dos tipos de servicios: con conexión y sin conexión, ambos parecidos a su similar en la capa de red, pero en éste caso los servicios son proporcionados a la capa de sesión, para que ésta a su vez se comuniquen con la capa de presentación.

2.6.4.2 Primitivas del servicio de transporte OSI

Las primitivas de la capa de transporte se dedican a proporcionar un servicio libre de errores, lo cual, debido a que la red no es muy confiable, es algo indispensable para llevar una comunicación correcta de principio a fin. Para esto las primitivas que se utilizan son:

a) Para un servicio orientado a conexión

- Petición de conexión
- Indicación de conexión
- Respuesta de conexión
- Confirmación de conexión
- Petición de desconexión
- Indicación de desconexión
- Petición de datos
- Indicación de datos
- Petición de datos enviados
- Indicación de datos enviados

b) Para un servicio no orientado a conexión

- Petición de datos
- Indicación de datos

2.6.4.3 Direccionamiento

El direccionamiento por lo general se realiza mediante un servidor de directorio, el cual contiene la dirección lógica de cada nodo que proporciona un servicio, llamada Punto de Acceso al Servicio de Transporte, o TSAP (*Transport Service Access Point*), junto con su nombre de servicio. Cuando un dispositivo quiere contactar un servicio lo hace por medio de su nombre, realizando una conexión con el servidor de directorio, quien a su vez realiza una nueva conexión entre el TSAP que corresponde al servicio solicitado y el TSAP del nodo que lo requiere. Una vez realizada la conexión entre el nodo solicitante y el nodo que alberga el servicio solicitado, la conexión entre el nodo solicitante y el servidor de directorio se libera.

Esta forma de direccionamiento requiere que cada nuevo servicio sea registrado para poder realizar la conexión.

2.6.4.4 Establecimiento de la conexión

Establecer y mantener una conexión es responsabilidad de la capa de transporte contemplando la solución a algunos problemas que se presentan frecuentemente como pueden ser:

- Pérdida de TPDU's.
- Retraso en la entrega de TPDU's.
- Duplicidad de los TPDU's.
- Reinicio súbito de la conexión.

2.6.4.5 Liberación de la conexión

Liberar la conexión es más sencillo que establecerla. La liberación de la conexión plantea un formato de ida-vuelta-ida, en el cual la petición de desconexión la realiza el emisor, el receptor responde con una confirmación de desconexión y se inicia un temporizador. Al momento de que el emisor recibe la confirmación, envía otra confirmación y la conexión se libera. En caso de no recibirse esta confirmación o la petición de enviar más datos, si el plazo del temporizador expira, la conexión se libera.

2.6.4.6 Multiplexión

En las redes que utilizan circuitos virtuales cada una de las conexiones de transporte utiliza una conexión de red. Una conexión de transporte consume recursos en los nodos de conmutación cuando no se está utilizando y no ha sido liberada y aunque sólo reserva espacio éste se desperdicia. Por este motivo es útil hacer uso de la multiplexión de conexiones de transporte sobre una sola conexión de red.

2.6.5. Capa de sesión

Esta capa tiene como objetivo controlar la sesión entre dos nodos que intercambian datos y su función es establecer la sesión, llevar el control de cuál nodo envía y cuál recibe los datos; en caso de alguna interrupción en la transmisión la capa de sesión debe reanudarla y finalizarla una vez que la transmisión ha concluido.

2.6.5.1 Administración de diálogo

En el modelo OSI se considera que el modo de transmisión de datos es full-dúplex para que los nodos que requieren compartir información lo puedan hacer al mismo tiempo. Al iniciar una sesión entre dos nodos y para aquellos que no tienen la capacidad de manejar el modo full-duplex, la capa de sesión da el permiso de envío a un nodo primero y después al otro.

2.6.5.2 Sincronización e Intercambio de datos

Otra tarea que corresponde a la capa de sesión es la sincronización, que consiste en llevar los valores de sesión al último estado conocido, previamente guardado, que se genera automáticamente mientras la sesión esté activa. En caso de haber perdido datos desde y en las capas superiores, puede ser de gran ayuda reestablecer los últimos valores conocidos.

El intercambio de datos entre la capa de transporte y la de presentación es una de las tareas más importantes para la capa de sesión, debido a que esta capa es la que las comunica y, como mediador, muchas veces pasa las peticiones invocando a las respectivas primitivas de cada capa.

2.6.5.3 Notificación de excepciones

Otra de las tareas de la capa de sesión es la notificación de errores inesperados. En caso de que un nodo tenga algún problema se puede notificar al nodo con el que se está comunicando que ha habido un problema. Otro caso es cuando se presentan reportes por problemas con las capas inferiores a la de sesión, o en caso de un error interno en la capa de sesión éste se le indica al usuario para que decida qué acción tomar.

2.6.5.4 Primitivas del servicio de sesión

Las primitivas de servicio de la capa de sesión se pueden clasificar en siete grupos:

- Establecimiento de conexión.
- Liberación de conexión.
- Transferencia de datos.
- Administración de testigos.
- Sincronización.
- Sincronización de actividades.
- Notificación de excepciones.

Estos grupos están dedicados específicamente a algunos servicios de esta capa.

2.6.6. Capa de presentación

La capa de presentación se encarga de presentar los datos a la capa de aplicación, debido a que cada equipo que envía datos tiene diferentes representaciones internas como pueden ser caracteres, números, archivos de sonido, video e imágenes, y el nodo que recibe los datos debe ser capaz de presentarlos como datos reconocibles al ser decodificados.

2.6.6.1 Criptografía y compresión de datos

Cuando un nodo cualquiera requiere enviar datos a otro se presenta un problema con la cantidad de datos que puede enviar, ya que conectarse a una red implica un costo dependiendo del ancho de banda contratado (512 kbps o 1Mbps, etc). Debido a esto es conveniente que los datos se compriman antes de ser enviados para aprovechar la velocidad de transmisión.

La capa de presentación también se debe encargar del cifrado de datos, de tal forma que la información entre los nodos no pueda ser obtenida por equipos externos. El proceso de cifrado de información consiste en alterar el contenido de la información, que en un principio es clara y entendible, de manera que al aplicarle una codificación ya no resulte entendible. Para poder convertir la información de nuevo a su estado inicial se utiliza una clave o llave, que permite aplicar el proceso inverso sobre los datos cifrados y obtener la información original.

2.6.6.2 Primitivas del servicio de presentación OSI

Las primitivas de servicio de la capa de presentación son usadas para comunicarse con la capa de aplicación y la de sesión, estas primitivas se dividen en varios grupos, para el caso de las primitivas orientadas a conexión, dichos grupos son:

- Establecimiento de conexión.
- Liberación de conexión.
- Transferencia de datos.
- Administración de testigos.
- Sincronización.
- Administración de actividades.
- Notificación de excepciones.
- Cambio de contexto.

Para servicio sin conexión solo existe una primitiva que es:

- Transferencia de datos.

2.6.7. Capa de aplicación

La capa de aplicación es la que proporciona las aplicaciones de usuario y del sistema y define que protocolos se utilizan para intercambiar datos.

Los protocolos de la capa de aplicación de ARPANET son los que más se usan en todo el mundo, ya que se han ido construyendo dependiendo de las necesidades prácticas que han ido surgiendo. De esta forma, a cada protocolo se le han ido agregando nuevas características hasta tener una gran gama de elementos para manejar las situaciones que requieren los usuarios. Por el contrario, los protocolos del modelo OSI se han creado con poca o nula experiencia práctica e incluyen características que pueden tener una aparente funcionalidad teórica. El problema con los protocolos de aplicación del modelo OSI es que las especificaciones en ocasiones son tan extensas y/o complejas que es prácticamente imposible su implementación. La mayoría de las implementaciones de protocolos de la capa de aplicación están hechas sin tomar en cuenta los protocolos del modelo OSI, aun cuando éstas sean normas ISO como el MOTIS para correo electrónico o el FTAM para transferencia de archivos. En su lugar se prefiere SMTP y FTP de ARPANET para correo electrónico y transferencia de archivos respectivamente.

Otra desventaja de OSI es que no maneja una implementación o especificación de un protocolo equivalente al HTTP de ARPANET.

Los servicios que proporcionan los protocolos del modelo OSI están especificados de una manera semi formal, indicando la funcionalidad que proporcionan, lo cual es una ventaja respecto a ARPANET, dado que ésta carece de especificaciones de servicio.

2.7 Norma IEEE 802 para redes de área local

Para establecer un acuerdo entre las partes que desean compartir información en una red, organizaciones internacionales han credo normas que deben seguir los participantes de la comunicación para poder entenderse. Existen diferentes recomendaciones, normas, estándares y protocolos escritos para las diferentes etapas de la comunicación. Los aspectos de la capa física y la subcapa de acceso al medio se encuentran definidos en la norma IEEE 802.3, comúnmente llamada Ethernet. Cabe aclarar que Ethernet y la norma IEEE 802.3 difieren ligeramente, aunque los términos se utilicen indistintamente. La norma IEEE 802.3 no es la única que estandariza el funcionamiento de la capa física y de enlace de datos, pero es ampliamente usada en muchos dispositivos y sistemas de comunicaciones, por lo que es una buena opción para implementar aplicaciones que se puedan o deban conectar con diferentes dispositivos.

La norma de la IEEE 802 se divide en varias secciones, tres de las cuales describen las normas para redes de área local, la 802.3 “Ethernet”, la 802.4 “Paso de testigo en Bus” y la 802.5 “Paso de testigo en anillo”. A continuación se explica más a detalle la norma IEEE 802.3 ya que sólo nos interesa la norma que trata de redes Ethernet para el desarrollo del sistema planteado en el Capítulo 1.

2.7.1. La norma 802.3

La norma 802.3 Ethernet utiliza la codificación Manchester para transmitir los datos a nivel físico. Establece el uso de cables como medio físico, cuya longitud es importante así como los conectores que se utilizan.

Las redes LAN que siguen la norma 802.3 se clasifican según algunos criterios como su velocidad de transmisión en Mbps (mega bits por segundo), el tipo de banda (banda ancha o banda base) y el tipo de cable o su longitud en metros. Se utiliza el siguiente formato para indicar las características de la red:

[Velocidad de transmisión en Mbps] – [Banda (base o ancha)] – [Longitud (en metros) o tipo de cable]

De esta forma una red del tipo LAN con banda base a 10 Mbps que utiliza cable UTP se designa como 10–BASE–T (la T refiere al par trenzado). En la Tabla 2-2 se presentan algunos datos para las diferentes especificaciones de la norma 802.3 y una velocidad de transmisión de 10 Mbps.

Tabla 2-2 Generalidades de la norma 802.3

	10Base5	10Base2	10Base–T	10Base–FL
Cable	Coaxial grueso	Coaxial delgado	UTP Cat 3/5	Fibra 62.5/125 micras
Pares	1	1	2	2
Full dúplex	No	No	Sí	Sí
Tipo Conector	N	BNC	RJ–45	ST
Topología	Bus	Bus	Estrella	Estrella
Longitud del cable	500 - 2500 m	185 - 925 m	100 - 500 m	2 km
Nº Nodos por segmento	100	30	1024	1024

En el nivel de enlace de datos para el control de acceso al medio esta norma utiliza el método de Detección de Portadora con Detección de Colisiones CSMA/CD Persistente–1.

2.7.2. Direcciones Físicas

En la capa de enlace de datos se utilizan direcciones físicas para acceder a los dispositivos que forman parte de una red física. En el estándar 802.3 estas direcciones reciben el nombre de direcciones de Control de Acceso al Medio, o direcciones MAC, también se les puede llamar de manera general direcciones físicas.

Las direcciones MAC son valores de 48 bits que identifican de manera única a cada dispositivo incorporado a una red. Se escribe en un formato de 12 números hexadecimales agrupados en pares, de tal manera que cada par forma un byte. En el caso de una red local, el administrador puede asignar las direcciones MAC

siempre y cuando ninguna dirección se repita. Cada dispositivo diseñado para conectarse a una red posee una dirección física única en todo el mundo, la cual se encuentra grabada en el dispositivo y no es posible cambiarla. Las direcciones físicas las debe asignar la *Autoridad de Registros Ether Type* del *Instituto de Ingenieros Eléctricos y Electrónicos* (IEEE). Esta institución asigna la parte más alta de la dirección MAC, es decir, los 24 bits más significativos. A esta parte de la dirección se le denomina *Identificador Único Organizacional (OUI)*. Los 24 bits más bajos los asigna el fabricante de los dispositivos, a manera de un número de serie.

Existen diferentes tipos de direcciones MAC, denominadas direcciones *unicast*, *multicast* y *broadcast*. Las direcciones *unicast* son las direcciones individuales que poseen los dispositivos. Las direcciones *multicast* hacen referencia a grupos formados dentro de la red por varios dispositivos, cada grupo se identifica con una dirección multicast y los dispositivos que quieran pertenecer a él se deben registrar como integrantes del grupo. La dirección *broadcast* es un caso particular de grupo multicast, al cual pertenecen todos los dispositivos de la red. El direccionamiento broadcast se utiliza cuando se requiere enviar un mensaje a todos los elementos conectados a la red, en este caso, en vez de enviar el mensaje individualmente a cada nodo, se utiliza la dirección broadcast.

Para identificar las direcciones individuales de las direcciones grupales se emplea el bit menos significativo del byte más significativo de la dirección MAC, si este bit es 0, se trata de una dirección individual (*unicast*) y si es un 1 entonces la dirección es grupal (*multicast*). La dirección FF FF FF FF FF FF (todos los bits iguales a 1) se reserva para dirección broadcast.

La transmisión de la dirección física se hace desde el byte más significativo hasta el byte menos significativo; sin embargo el orden de transmisión de cada byte es del bit menos significativo hasta el más significativo.

2.7.3. Formato de las tramas físicas

El formato de una trama Ethernet se muestra en la Figura 2.16.



Figura 2.16 Formato de una trama Ethernet

A continuación se describe el contenido de cada campo de una trama Ethernet.

Preámbulo. Tiene la longitud de siete bytes, sirve para sincronizar el medio físico y es una secuencia alternada de unos y ceros cuya codificación Manchester genera una onda cuadrada que sincroniza los relojes del receptor y el emisor.

Delimitador de inicio. A este campo se le denomina SFD (*Start Frame Delimiter*). Está formado por un byte e indica el inicio de la trama con el patrón binario 10101011. Los tres campos siguientes forman el encabezado de la trama Ethernet.

Dirección destino. Dirección MAC a la que va dirigida la trama.

Dirección de origen. Dirección MAC del nodo que envía la trama.

Longitud. El campo *tipo/longitud* consta de dos bytes y puede tener dos significados diferentes. La longitud máxima del campo de datos de una Ethernet es de 1500 bytes, por lo tanto si el valor contenido en el campo *tipo/longitud* es igual o menor a 1500, este valor indica la cantidad de bytes contenidos en el campo de datos. Si es mayor a 1536, el valor de este campo se refiere al tipo de paquete del que se trata. El tipo, o ethertype, es un código que corresponde a un protocolo de la capa superior al cual va destinado el paquete. Si el valor de este campo está entre 1501 y 1535 el paquete no es válido.

Datos. Es la información que proviene de las capas superiores y puede contener de 46 a 1500 bytes.

Relleno. Si los datos ocupan 46 bytes o menos, el campo se rellena para tener el tamaño mínimo requerido.

Secuencia de verificación. Se le llama comúnmente FCS (*Frame Check Sequence*). Es un número de cuatro bytes que se añade para verificar la integridad de los datos enviados y recibidos. Este número es calculado por el emisor basado en el contenido de la trama (sin contar el preámbulo ni delimitador de inicio) y lo envía como parte de la trama. Al llegar la información a su destino, el receptor calcula de nuevo el número y lo compara contra el contenido del campo *Secuencia de Verificación*; si ambos valores coinciden, los datos no sufrieron alteraciones o pérdidas en el camino, pero si son diferentes, entonces la información llegó alterada y no corresponde a los datos que originalmente fueron enviados.

La longitud máxima de una trama Ethernet es de 1518 bytes y la mínima es de 64 bytes, desde el campo *Dirección de Destino*, hasta el campo de *Secuencia de Verificación*. Si se intenta transmitir una trama que no cuente con el número mínimo de bytes especificado, el campo de datos se debe rellenar con ceros hasta que la longitud alcance el valor mínimo. Cuando este paquete se recibe en la máquina de destino, los ceros de relleno son descartados.

Existen tramas que contienen información de control en lugar de datos, por ejemplo para implementar el control de flujo en la capa de enlace, enviando una trama de pausa que le indica al emisor que detenga su actividad durante el tiempo contenido en la trama.

Para identificar a una trama de control de una de datos, el valor del campo *tipo/longitud* debe estar fijado en 0x8808 (hexadecimal). En los dos primeros bytes del campo de datos se indica un código de operación que corresponde a la acción de control. La solicitud de una trama de pausa se indica con el código 0x0001 y en los siguientes dos bytes se especifica la duración de la pausa. El valor del tiempo de pausa abarca desde 0x0000 hasta 0xFFFF y las unidades son 512 tiempos de bit (es decir, un tiempo de pausa con valor de 0x0001 tiene la duración de 512 bits).

Una trama de pausa puede tener en el campo *Dirección de Destino* el valor de 01-80-C2-00-00-01, o bien, la correspondiente dirección de destino. En la Figura 2.17 se muestra la estructura de una trama de pausa.

Preámbulo	SFD	Dirección Destino	Dirección Origen	Tipo/Longitud	Código de Operación MAC	Parámetros de Control MAC	Reservado	FCS
7 bytes	1 byte	6 bytes = (01-80-C2-00-00-01) o dirección de destino	6 bytes	2 bytes = Control MAC (88-08)	2 bytes = (00-01)	2 bytes = (00-00 a FF-FF)	42 bytes = todos ceros	4 bytes

Figura 2.17 Formato de una trama de pausa

La norma 802.3 también ha considerado mejoras para Ethernet, como lo sugiere la norma 802.3u para *Fast Ethernet* y varias normas para velocidades de transmisión en gigabits por segundo englobadas en el estándar *Gigabit Ethernet*.

Fast Ethernet opera en banda base a velocidades de 100 Mbps, utiliza cable UTP o fibra óptica para la transmisión de datos. *Gigabit Ethernet* opera en banda base a velocidades de 1 y 10 Gbps, utiliza cable UTP, STP o fibra óptica como medio de transmisión. Tanto *Fast Ethernet* como *Gigabit Ethernet* utilizan el método CSMA/CD para el acceso al medio.