

TEMA 1 INTRODUCCIÓN

1.1 Evolución histórica de las telecomunicaciones

Un sistema de telecomunicación se puede definir como los medios necesarios para emitir o recibir datos de cualquier naturaleza entre dos sistemas geográficamente separados.

Nos vamos a centrar en tres medios principalmente:

- intercambio de señales eléctricas a través de cables eléctricos.
- señales electromagnéticas a través del aire (o vacío).
- señales ópticas a través de conductores ópticos.

S. XVIII: Faraday introduce los principios de inducción electromagnética. Al mover un imán alrededor de un metal se genera una corriente.

S. XIX: Samuel Morse (telégrafo), 1844 alfabeto Morse. Aquí ya puede separarse el nivel físico (cable) y lógico (alfabeto). Las telecomunicaciones deben estar sistematizadas, emisor y receptor deben comprender el sistema para poder entenderse. El conjunto de normas que rigen la comunicación se denomina protocolo. Poco después se intentó hechar un cable entre América y Europa, aunque no llegó a cuajar (sólo funcionó 20 o 30 días).

Otro aspecto muy importante es la velocidad de transmisión. De las 10-12 palabras/minuto iniciales hemos pasado a miles de palabras/segundo.

- Maxwell (Teoría electromagnética de la luz). Estudio de ondas con comportamiento igual a la luz.
- Marconi (radiotelegrafía) 1896. Comunicación sin necesidad de un conductor físico. Se evoluciona hacia la transmisión de radio y telefonía.
- 1909 → USA primeras transmisiones de radio.
- 1927 → Primer enlace intercontinental mediante radio de onda corta. A continuación aparece la modulación en frecuencia o FM en 1933.
- 1937 → radar (teledetección).
- 1938 → Modulación PCM. Primera forma de modular información analógica a forma digital.
- 1941 → TV
- 1954 → TV color.
- 1957-58 → Satélites (Sputnik ruso), primer satélite de comunicaciones por parte de los americanos.
- 1960 → Láser (a través de fibra óptica).
- 1969 → Cobertura total de la superficie terrestre mediante satélites.
- 1977 → Primeros sistemas de telefonía mediante fibra óptica.

Una red informática es un conjunto de computadores autónomos interconectados capaces de intercambiar información. Computador autónomo es cualquier dispositivo capaz de procesar información. Con las redes se persigue:

- Intercambio de información.
- Compartir recursos.
- Mayor fiabilidad.
- Mayor versatilidad (más fácil ampliar el sistema).

Clasificación de las redes (según su distancia):

	Distancia	Nombre
Sistema	0.1 - 1 m.	multiprocesador
Sala edificio campus	10 m, 100 m, 1 km	LAN (Local Area Network)
Ciudad	10 km	MAN (Metropolitan)
País, continente	> 10 km	WAN

Estructura de una red

ARPANET evolución de DARPA NET que englobó a todas las universidades americanas. Embrión de Internet.

Las máquinas que conectadas a una red, ejecutan programas de usuario se conocen como host. Los hosts están conectados a través de una subred que es la encargada de las comunicaciones. Una subred contiene dos elementos distintos: líneas de comunicación y unos dispositivos denominados IMP'S (Internet Message Processor), computadores dedicados únicamente a tareas de comunicaciones. Hay dos tipos de diseño de redes: punto a punto (dos IMP que no comparten línea se comunican a través de otro IMP) y canales de difusión (todos los IMP comparten una única línea), el IMP tendrá que gestionar el acceso de los hosts a ese único canal de difusión.

Topología de red:

Canales punto a punto

- **Estrella:** todos los IMP se comunican a través de un IMP central. La fiabilidad de esta red es la del nodo central (es poco fiable).
- **Anillo:** la caída de un IMP no tiene porque impedir la comunicación de los demás.
- **Arbol:** característica en WAN
- **Completa:** todos los IMP están interconectados entre sí. Siempre está garantizada la comunicación.

Con canal de difusión

- **En bus:** la más conocida es Ethernet.
- **Anillo compartido.**

Las líneas de comunicación no tienen porque ser líneas físicas, pueden ser líneas de radio por ejemplo.

1.2 El modelo multinivel de ISO

El modelo surge como un medio de sistematización para la comunicación. Cada uno propuso un modelo, con la única característica común de una subdivisión en niveles por lo que surgió el modelo de referencia ISO para OSI, que se constituyó en un standard (OSI = interconexión de sistemas abiertos).

Organizaciones internacionales que se dedican a la estandarización en telecomunicaciones:

- ITU: unión internacional de telecomunicaciones.
- ISO: miembro del CCITT en comunicaciones.
- IEEE: redes de área local, norma 802.
- IAB: Internet Activity Board. Sólo se ocupa de la regulación de utilización en Internet.

El modelo multinivel de ISO se desarrolló a partir de 1983, su nombre completo es modelo ISO para la interconexión de sistemas abiertos. Modelo OSI de ISO.

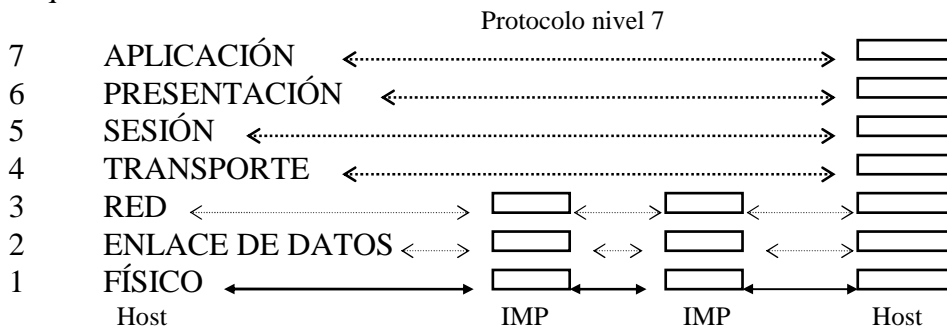
Para el diseño del modelo se siguieron 4 principios:

- Se creaba un nuevo nivel cada vez que se necesitaba un modo de abstracción distinto.
- Cada nivel realiza una tarea bien definida.
- La funcionalidad de cada nivel se fijó con vistas a definir protocolos internacionalmente estandarizados.
- El límite entre los niveles se fijó de manera que se minimizase el flujo de información entre ellos.

El modelo de referencia no es una arquitectura de red, no implica soluciones tecnológicas. Indica una funcionalidad para cada nivel pero no como solucionar los problemas.

Otra cosa que podemos extraer de los principios es que la información que intercambien los niveles sea la mínima posible.

Esquema con los 7 niveles del modelo de referencia:



El proceso de comunicación se lleva a cabo siempre en función del nivel en que nos encontremos.

El conjunto de normas que deben cumplir dos aplicaciones de nivel 7 para comunicarse es el protocolo nivel 7.

El nivel de aplicación se identifica con el tratamiento de datos.

El nivel de presentación se identifica con la interpretación de datos.

El nivel de sesión se identifica con los diálogos de control.

El nivel de transporte se identifica con la integridad de los mensajes.

El nivel de red se identifica con el encaminamiento.

El nivel de enlace se identifica con la detección y control de errores.

El nivel físico se identifica con la conexión de equipos.

El **nivel físico** define las especificaciones eléctricas, mecánicas, procedurales y funcionales del enlace físico entre sistemas. Características que preocupan: niveles de tensión, los conectores a emplear, tiempo de transición entre cambios de nivel, tipos de conductores de la información, velocidad de transmisión, distancia máxima del enlace. El nivel físico trabaja con bits.

El **nivel de enlace** de datos, su misión es proporcionar al nivel superior un canal físico fiable para la transmisión de datos. Intenta detectar y corregir los errores. Otra función de este nivel es el control de flujo, trata de evitar que no se manden datos a una velocidad mayor de la que el receptor es capaz de recibir. También agrupa la información en tramas (agrupación de bits) que es la unidad con la que trabaja.

El **nivel de red** se encarga de la operación de la subred, su principal misión es el encaminamiento, esto origina el problema de la congestión que también trata de corregir este nivel. Para evitar esto hay unos algoritmos que controlan la congestión. Trabaja con paquetes. El encaminamiento determina el camino que debe seguir la información del host origen al host destino.

El **nivel de transporte** se encarga de separar los niveles superiores de la cambiante tecnología de los niveles inferiores. Otra función de este nivel es multiplexar de modo transparente para los niveles superiores varias conexiones de transporte sobre una misma conexión de red. Lo que proporciona es una conexión extremo a extremo libre de errores y que proporciona los datos a la recepción en el mismo orden en que se han originado en la emisión. Este nivel controla los errores que se pueden producir a través de una subred a diferencia del nivel de enlace que controla los errores que se producen en un enlace físico (un cable). Este nivel trabaja con mensajes.

El **nivel de sesión** se dedica a establecer, finalizar y gestionar las sesiones de diferentes máquinas. Una sesión es el diálogo entre dos o más entidades.

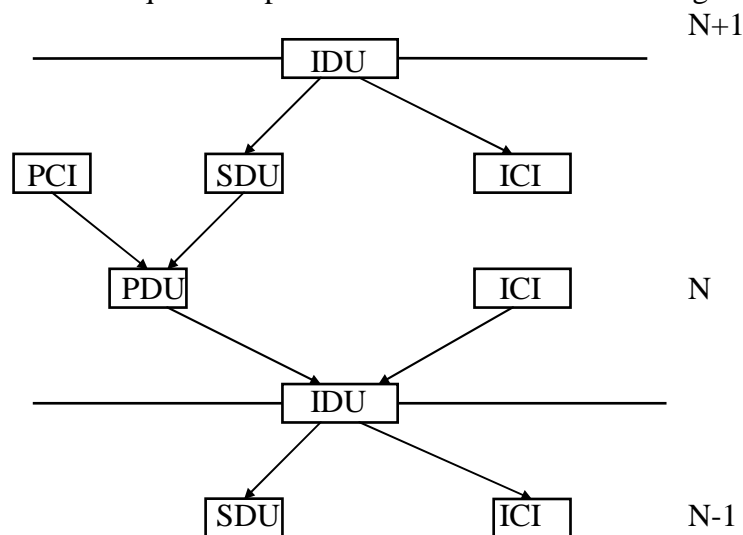
El **nivel de presentación** se encarga de la interpretación de los datos, que la información que envía un sistema sea legible por el sistema interlocutor de éste. También encripta los datos y los comprime.

El **nivel de aplicación** es el más próximo al usuario e incluye una serie de protocolos para uso común como mensajería electrónica, ...

Un nivel es un suministrador de servicios, que consta de varias funciones. Una función es un concepto abstracto que sirve para definir un subsistema que forma parte de un nivel.

Una entidad es un elemento activo de un nivel, lleva a cabo e implementa las funciones de un nivel. Las primitivas son operaciones disponibles para acceder a un determinado servicio.

La información que se va pasando nivel a nivel se divide según el siguiente esquema:



SDU = Service Data Unit (unidad de datos de servicio), esos datos son los transferidos del nivel N+1 al nivel N.

PCI = (Información de control de protocolo), se intercambia entre entidades del mismo nivel en máquinas distintas.

PDU = (Unidad de datos del protocolo), está formada por los datos que le ha pasado el nivel superior a ese nivel para transferir.

ICI = (Información de control del interface), indica lo que espera el nivel superior de él.

IDU = (Unidad de datos del interface).

Cada vez que se intercambia información entre los niveles se añade información.

El servicio define las operaciones que el nivel es capaz de llevar a cabo para sus usuarios (niveles superiores) pero sin indicar como hacerlo. Los protocolos indican como hacerlo.

Lo que caracteriza a un servicio es su calidad o su fiabilidad. Tendremos 2 tipos de servicios:

- *con conexión*: es necesario establecer previamente a la transferencia de transmisión un camino para llevarla a cabo.

Ventaja: la información llega en el mismo orden en que fue enviada (teléfono).

- *sin conexión*: no hay búsqueda previa de un camino, sino que la información se divide en unidades, las cuales se transmiten independientemente, pudiendo seguir cada una un camino diferente.

Ventaja: no se pierde tiempo en buscar un camino, estos servicios son mucho más versátiles (correo).

Servicio con conexión fiable: emulación de terminal.

Servicio con conexión no fiable: transmisión de voz digitalizada.

Servicio sin conexión fiable: mensajería electrónica con acuse de recibo.

Servicio sin conexión no fiable: mensajería electrónica.

1.3 Tipos de redes

Redes públicas: el usuario debe abonarse para recibir los servicios. PSTN, PSDN, ISDN.

Para optar por un tipo de red u otro se deberá tener en cuenta los siguientes factores:

- naturaleza.
- dimensión de la red.
- separación física entre las máquinas.

Interconexión de dos PC's en la misma sala

- cable serie, el subsistema de comunicaciones UART.
- red local.

Dos PC's físicamente distantes

Uso de una red pública de cualquier tipo. El subsistema de comunicaciones los constituirán el modem o la tarjeta RDSI.

TEMA 2 EL NIVEL FÍSICO

2.1 Fundamentos teóricos de la transmisión de datos

Los medios de transmisión se pueden clasificar en medios guiados y medios no guiados:

- *Guiados*: las ondas se transmiten confinándolas dentro del medio de transmisión a lo largo de todo su camino (pares de cobre, cables metálicos, cables fibra óptica).
- *No guiados*: las ondas electromagnéticas que circulan por ellos no se encauzan sino que se propagan a través del aire, agua e incluso el vacío (transmisiones de radio).

Todas las señales que se pueden intercambiar entre dos puntos se denominan ondas electromagnéticas, que se pueden agrupar en función del tiempo y en función de la frecuencia.

Dentro del dominio temporal, las ondas pueden ser:

- *continuas*: la intensidad de la señal varía suavemente en el tiempo sin presentar saltos ni discontinuidades.
- *discretas*: la intensidad se mantiene constante durante un determinado intervalo de tiempo, transcurrido el cual la señal varía a otro valor constante.

El tipo de señales periódicas se caracterizan por tener un patrón que se repite a lo largo del tiempo. $s(t)$ es periódica si $s(t+T) = s(t) \quad -\infty < t < +\infty$

En estas señales nos basaremos para estudiar las ondas electromagnéticas. La onda que nos va a servir de base será la onda senoidal:

$$s(t) = A \operatorname{sen} \left(\frac{2\pi}{T} t + \Phi \right) = A \operatorname{sen} (2\pi f t + \Phi)$$

A = (amplitud), valor máximo de la función $s(t)$

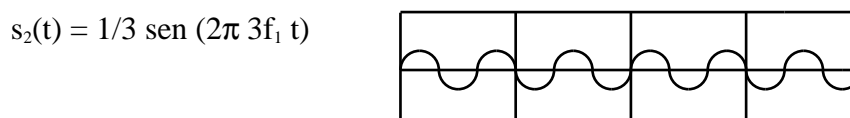
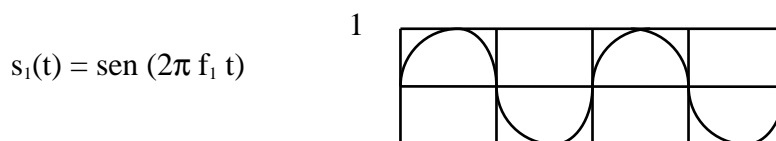
$f = 1/T$ (frecuencia), razón de repetición de la señal a lo largo del tiempo).

Φ = (fase de la señal), posición relativa de la señal dentro del periodo.

λ = (longitud de onda), indica la distancia que recorre la señal a lo largo de un periodo.

$$\lambda = v T \quad \text{donde } v \text{ es la velocidad de propagación; } \quad v_{\text{luz}} = 3 \times 10^8 \text{ m/s}$$

En la práctica una señal electromagnética puede tener componentes de muchas frecuencias.



Cuando todos los componentes de una señal tienen frecuencias múltiplo de una dada, a ésta se le conoce como frecuencia fundamental. La inversa de esta frecuencia fundamental será el periodo de la onda compuesta.

Mediante el análisis de Fourier se demuestra que cualquier señal está constituida por componentes senoidales de distintas frecuencias.

Se define como espectro de una señal el conjunto de frecuencias que la constituyen.

Para la señal $s(t) = \sin(2\pi f_1 t) + 1/3 \sin(2\pi 3f_1 t)$, el espectro de $s(t)$ está entre f_1 y $3f_1$

El ancho de banda de una señal es el ancho del espectro $BW = 3f_1 - f_1 = 2f_1$

El ancho de banda eficaz es el que comprende las frecuencias dentro de las cuales la señal aglutina más energía. Si una señal contiene una componente de frecuencia 0, se dice que la señal tiene componente continua.

El ancho de banda es importante porque cada medio de transmisión actúa como un filtro que sólo deja pasar unas determinadas frecuencias (ancho de banda del canal)

Canal $BW = 4 \text{ Mhz}$ $s(t) = \sum_{K=1}^{\infty} \sin(2\pi K f_1 t)$

Vamos a aproximarla a la señal pulso cuadrado por sus tres primeras componentes

$s'(t) = \sin(2\pi f_1 t) + 1/3 \sin(2\pi 3f_1 t) + 1/5 \sin(2\pi 5f_1 t)$ $BW's = 5 f_1 - f_1 = 4 f_1$

Equiparando el ancho de banda de la señal con la del canal tenemos que

$4 f_1 = 4\text{Mhz}$ $f_1 = 1\text{Mhz}$

$T = 1/ f_1 = 1/10^6 = 1\mu\text{seg.}$

Se transmiten 2 bits por periodo en una señal pulso cuadrado. La velocidad máxima en este canal será 2 Mbits/s

Ejemplo

Canal con $BW = 8\text{Mhz}$

$4 f_1 = 8\text{Mhz}$ $f_1 = 2\text{Mhz}$

$T = 1/ f_1 = 1/2 \times 10^6 = 0.5\mu\text{seg.}$ La velocidad máxima en este canal será 4 Mbits/s

Doblando el ancho de banda del canal hemos conseguido doblar la velocidad.

- Considerando el mismo ancho de banda del canal pero la aproximación:

$s'(t) = \sin(2\pi f_1 t) + 1/3 \sin(2\pi 3f_1 t)$

$BW's = 3f_1 - f_1 = 2f_1$ $2f_1 = 8 \text{ Mhz}$ $f_1 = 4 \text{ Mhz}$

$T = 1/ f_1 = 1/4 \times 10^6 = 0.25\mu\text{seg.}$ La velocidad máxima en este canal será 8 Mbits/s

Este aumento de velocidad se debe a una peor aproximación de la señal, esto puede ser peligroso si los que vayan a leer la señal no pueden distinguir si es 0 o 1.

A lo largo del camino que debe recorrer la señal sufre una serie de perturbaciones. Estas perturbaciones pueden ser tres, básicamente:

- *Atenuación*, es la pérdida de energía que sufre la señal en el camino que recorre entre el emisor y el receptor. Lo sufren todas las señales.
- *Distorsión de retardo*, es un fenómeno característico de los medios guiados y está causada por el hecho de que la velocidad de transmisión varía con la frecuencia. Entonces una señal compuesta por varias frecuencias, cada componente puede sufrir un retardo respecto a las otras.
- *Ruido*, son señales no deseadas que se suman a la señal transmitida.

Señal recibida = Señal emitida atenuada y distorsionada + señales no deseadas (ruido)

El ruido es el factor de mayor importancia. Existen diferentes tipos de ruido:

- *Ruido térmico*, se debe a la agitación térmica de los electrones en el conductor. Está presente en todos los dispositivos.
- *Ruido de intermodulación*, causado por el hecho de transmitir señales de distinta frecuencia sobre el mismo medio.
- *Diafonía*, ruido debido al acoplamiento entre señales que circulan por conductores próximos.
- *Ruido impulsivo*, es difícil eliminarlo. Está constituido por picos o pulsos irregulares de corta duración y gran amplitud. No afectan por igual a las transmisiones analógicas que a las digitales, en las cuales es el principal problema. Transmitiendo a 4800 bps un pico de 0.01 seg. puede estropear 48 bits de información.

Los 3 primeros tipos de ruido son previsible y subsanables de alguna manera.

2.2 Los medios de transmisión

Capacidad del canal: capacidad para transportar información. Relacionado con esto está el ancho de banda, que se mide en hertzios.

Capacidad digital del canal o tasa / razón de bits: es la cantidad de bits que puede transportar el canal por unidad de tiempo, se mide en bits por segundo.

Otro concepto que va a condicionar la capacidad del canal será el ruido. Nos interesará saber la cantidad de ruido que sufrirá la información en ese canal. Siempre existirá. En los canales digitales nos interesará un parámetro originado por el ruido, que es la tasa de errores.

Se deberá conseguir la mayor tasa o razón de bits posibles con la menor tasa de errores.

El espectro electromagnético divide las frecuencias según su uso. Cada rango de frecuencias se utiliza para una cosa.

Medios guiados

La capacidad del canal depende de dos factores:

- de la distancia del enlace.
- será mayor si el enlace es punto a punto que si es multipunto.

CABLE DE PAR TRENZADO: es el medio más común para la transmisión de datos. Consiste en dos cables de cobre embutidos en un aislante y entrecruzados en forma de espiral. Cada uno de estos pares es un enlace. Se trenza para evitar la diafonía entre pares próximos. Normalmente se encuentran 4 enlaces dentro de una manguera.

- *Aplicaciones*: sirve para transportar señales tanto analógicas como digitales, se usa mucho en telefonía sobre todo para el bucle de abonado, también se usa mucho en redes de área local.

- *Características de transmisión*: tienen mucha susceptibilidad al ruido, se debe emplear en distancias cortas sobre todo para altas velocidades de datos.

- *Capacidad de transmisión*: soportan un ancho de banda de 250 KHz y la razón de bits oscila entre 4-100 Mbps

A mayor velocidad de transmisión, menor longitud.

Normalmente el cable de par trenzado se presenta de 2 maneras:

- a) (sin apantallar) UTP (Unshielded Twisted Pair). El estándar EIA-518-A clasifica los cables en 5 categorías, los de transmisión de datos son:

- Categoría 3: velocidad hasta 16 Mbps
- Categoría 4: velocidad hasta 20 Mbps
- Categoría 5: velocidad hasta 100 Mbps

Lo que marca la categoría del cable es la calidad del trenzado.

b) STP apantallado o trenzado (Shielded Twisted Pair), cada par de conductores se recubre de una malla aislante. Da mejores resultados en la transmisión pero es más caro.

CABLE COAXIAL: consta de dos conductores, uno interno llamado núcleo y otro externo en forma de malla que rodea el núcleo. Están separados por un dieléctrico y por encima de la malla hay una funda protectora. Tiene un diámetro que va desde 0.5 a 2.5 cm.

El hecho de disponer así los conductores permite al cable transportar un mayor rango de frecuencias y a mayores distancias que el cable de par trenzado.

- *Aplicaciones:* televisión, tv por cable, interconexión de centrales en telefonía, interconexión de periféricos a computadores, redes de área local.

- *Características de transmisión:* transmite señales analógicas y digitales, es más inmune que el par trenzado a las interferencias eléctricas y a la diafonía. Puede transmitir hasta 400 Mbps.

FIBRA ÓPTICA: conduce señales de naturaleza luminosa. Es una fibra de vidrio o plástico extremadamente fina y flexible. Está formada por 3 secciones concéntricas: un núcleo que permite circular la luz, un revestimiento con propiedades ópticas distintas al núcleo y la cubierta de protección contra factores ambientales. Poco peso y pequeño tamaño.

- *Aplicaciones:* permiten transmitir datos con velocidades de hasta 2 Gbps. Al transmitir señales luminosas es inmune a señales eléctricas exteriores y como no radia energía electromagnética es más difícil pinchar una línea.

Se utiliza en telefonía para el enlace entre centrales y para la interconexión de redes de área local (redes tipo campus).

Utiliza frecuencias entre 10^{14} y 10^{15} Hz. Para transmisión se requiere una fuente de luz, el medio que es la fibra y un receptor de luz. La fuente de luz suele ser un diodo LED o un rayo láser, mientras que el receptor suele ser un fotodiodo.

La fuente de luz vierte los rayos en la fibra con una cierta inclinación, esta luz se va reflejando en la fibra y transmitiendo. La luz que se refleja en la fibra con menor grado de inclinación que el crítico se absorbe.

Medios no guiados

Distinguiremos 4 tipos de señales que sirven para transmisiones inalámbricas:

- Microondas terrestres.
- Microondas vía satélite.
- Ondas de radio.
- Infrarrojos.

Todos los medios de este tipo se caracterizan porque usan antenas. En la transmisión la antena radia energía electromagnética en el medio y para la recepción las antenas captan la energía electromagnética presente en su entorno.

Existen dos configuraciones para la transmisión inalámbrica:

- **Direccional:** se concentra la energía en un haz y para su correcta propagación la antena del emisor y la del receptor deben estar alineadas.
- **Omnidireccional:** el diagrama de radiación de la antena es disperso.

A mayores frecuencias es más fácil concentrar toda la energía en un haz, en una dirección.

Microondas, 2 Ghz - 40 Ghz, se pueden conseguir haces altamente direccionables.

Ondas de radio, 30 Mhz - 1 Ghz, normalmente transmisión omnidireccional.

Infrarrojos, 3000 Ghz - 20000 Ghz, son direccionables pero se reflejan.

MICROONDAS TERRESTRES: usan antenas parabólicas que se deben colocar a alturas considerables. La distancia máxima entre los enlaces es: $d = 7.43 \sqrt{Kh}$ h = altura de la antena, K = 4/3, d está en kilómetros y h en metros.

Se usan en telefonía para enlaces entre centrales, para enlaces entre repetidores de tv y cada vez se usan más para interconexión de redes de área local.

Tanto las microondas como las ondas de radio tienen un problema, es que su uso está legislado por el gobierno. Las microondas terrestres son sensibles a las condiciones meteorológicas cambiantes (tormentas, lluvia).

Las características de transmisión varían según la frecuencia utilizada.

MICROONDAS VÍA SATÉLITE: utilizan para la retransmisión de la señal un satélite que está en órbita terrestre. El satélite recibe señales por su canal ascendente y las transmite por su canal descendente a otras estaciones. Estos dos canales operan en frecuencias diferentes para evitar las interferencias entre ellos.

Los satélites se usan tanto para enlaces punto a punto como para la difusión de señales.

La mayoría de satélites que se usan, están en una órbita geoestacionaria (siempre sobre el mismo punto de la tierra) a 35.784 km sobre la superficie terrestre. Además, la distancia entre dos satélites en el mismo plano es de al menos 4 grados.

Aplicaciones: difusión de televisión, telefonía enlaces a largas distancias, constitución de redes privadas.

El rango de frecuencias óptimo va desde 1 a 10 Ghz, de este rango se utiliza la banda que va de 4 a 6 Ghz. Para el enlace ascendente de 5.9 - 6.4 Ghz y para el descendente 3.7 - 4.2 Ghz, debido a la saturación de esta banda se empieza a usar la banda 10 / 12 Ghz.

Debido a la distancia entre la antena terrestre y el satélite, la velocidad de propagación de la señal sufre un retardo.

ONDAS DE RADIO: se caracterizan por ser omnidireccionales. Su utilización está regulada.

Los rangos de frecuencia a los que trabajan van desde 3 KHz a 1 Ghz.

Aplicación: radio, televisión.

Son sensibles a interferencias por condiciones climáticas adversas. Otra característica de transmisión que se emplea en algunos casos es la reflexión ionosférica.

INFRARROJOS: se basan en la transmisión y recepción de luz infrarroja, sirven para enlaces muy direccionables. Se emplean para transmisión dentro de la misma habitación ya que no pueden atravesar las paredes, aunque se reflejan.

Su principal ventaja para transmitir datos es que su uso no está controlado.

2.3 Transmisión analógica y digital

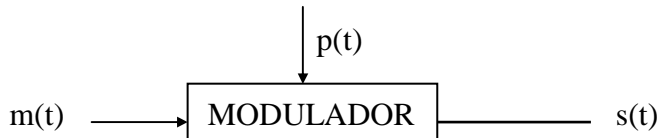
Modulación

La modulación sirve para adecuar las señales al medio físico sobre el que se transmiten.

Razones para modular datos analógicos:

- Cuando el medio físico por el que se van a transmitir es digital.
- Para hacer más efectiva la transmisión.
- Para poder compartir canales. (Se modula cada señal a una frecuencia y así se puede transmitir los datos de diferentes comunicaciones por un mismo canal).

La modulación se define como el proceso de combinar una señal de entrada $m(t)$ que aporta la información a transmitir (moduladora), con otra señal $p(t)$ denominada moduladora a frecuencia f_c , para producir una señal u onda llamada modulada, cuyo ancho de banda se reparte en torno a f_c .



La señal moduladora controla algún parámetro de la señal portadora. Los parámetros de la onda pueden ser: amplitud, frecuencia y fase.

Todo esto es aplicable tanto a señales analógicas como digitales.

Una señal que no se modula, se transmite en banda base.

Tipos de modulación en función de si la portadora y la moduladora son analógicas o digitales:

p(t)	m(t)	Modulación
Analógica	Analógica	AM (varía amplitud), FM (varía frecuencia), PM (varía fase)
	Digital	ASK (varía amplitud) FSK (varía frecuencia) PSK (varía fase)
Digital	Analógica	PAM (Pulse Amplitude Modulation) PDM (Pulse Duration Modulation) PPM (Pulse Position Modulation) PCM (Modul. por impulso modificado) δ

Modulación con portadora analógica y moduladora analógica

La señal portadora es una onda sinusoidal.

AM: el parámetro afectado es la amplitud.

FM: una onda modulada en frecuencia presenta una variación en su frecuencia proporcional a la amplitud de la moduladora.

FM es más inmune al ruido que AM ya que la información que transmite la lleva en la frecuencia y no en su amplitud como la AM. Aunque las señales AM tienen más alcance.

PM: la señal portadora sufre una variación en fase proporcional a la amplitud de la moduladora.

Modulación con moduladora digital y portadora analógica

ASK:

FSK:

PSK: cuando se produce un cambio en la moduladora de 0 a 1 (al inicio de cada periodo de bit) se produce un cambio de fase en $s(t)$.

Es uno de los tipos que más se emplea en los modems.

Modulación con portadora digital y moduladora analógica

La señal a transmitir será una onda discreta.

PAM: se fijan unos periodos de muestreo en los cuales se muestrea la señal y se cuantifica su valor.

En una primera fase se obtiene una muestra de la señal en el periodo de muestreo y en la segunda fase se da un valor a esa muestra.

Se debe muestrear la señal con un periodo de muestreo para que la señal no pierda información. Es importante elegir bien la frecuencia de muestreo.

Teorema de Nyquist

Muestreando con una frecuencia el doble de la frecuencia máxima de la señal se puede reconstruir sin pérdida de información.

En la PAM en muchos momentos no se transmite, por tanto se puede utilizar para transmitir otra señal en el mismo canal. Esta técnica se conoce como multiplexación por división en el tiempo.

PDM: la información la lleva la duración del pulso. Se divide el tiempo en intervalos de muestreo y también hay un tiempo para la cuantificación.

PPM: es idéntica a la PDM pero se marca con dos pulsos de pequeña duración el inicio y final de cada pulso PDM.

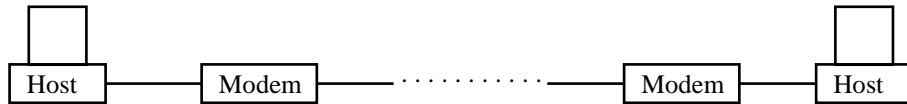
PCM: es muy similar a la PAM pero es binaria.

Mod. δ : trata de codificar la información de la señal moduladora en cada instante de muestreo en un solo bit.

Modems

Los modems sirven para adecuar las señales de transmisión al medio físico por el que van a transitar. Cualquier equipo que modula la señal para su transmisión y la demodula para su interpretación será un modem.

El esquema de un sistema de comunicación basado en modems será el siguiente:



Los equipos se suelen denominar DTE y el modem DCE

DTE = Data Terminal Equipment

DCE = Data Circuit Terminating Equipment

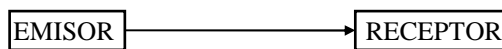
Interfaz normalizadas para la conexión entre el host y el modem (DTE - DCE) hay muchas, las más comunes son:

- ITU - T V.24 / V.28 (EIA RS-232)
- EIA RS-422
423
- V.35

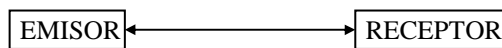
El interfaz DCE - DCE está descrito en las normas V, que definen como se establece la conexión entre un modem y el modem remoto (velocidad de transmisión, comunicación síncrona o asíncrona y los modos de explotación).

Los modos de explotación de un circuito son tres:

- **SIMPLEX:** constituye un canal unidireccional en el cual el flujo de información solo circula en un sentido. (Transmisión de TV)



- **SEMI-DUPLEX (HALF-DUPLEX):** la información circula en los dos sentidos pero nunca simultáneamente.



- **DUPLEX:** permite el tránsito de información en ambos sentidos simultáneamente. Es equivalente a dos simplex.



Los modems emisor y receptor deben ajustarse a una velocidad de transmisión, pero también deben saber dónde empieza un bit.

El modo de transmisión puede ser:

- **Síncrono:** el transmisor y el receptor trabajan independientemente el uno del otro e intercambian una señal al principio de cada señal.
- **Asíncrona:** la información se agrupa en caracteres y se coloca al inicio de esa secuencia, una secuencia de inicio y al final se pone una secuencia de final.



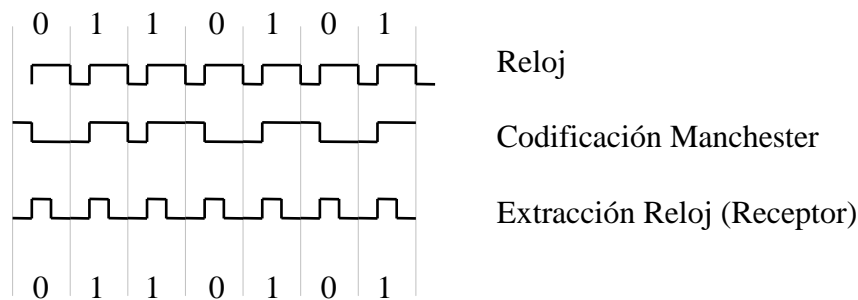
El bit de arranque es la secuencia de inicio. Cuando se acaban los bits de datos se devuelve la línea a su estado inactivo, este bit se denomina bit de parada.

En el modo síncrono emisor y receptor intercambian la señal de reloj, de esta forma ambos trabajan con la misma y permanecen sincronizados hasta el final de la comunicación.

Hay dos formas de conseguir esta sincronización:

- Usar líneas adicionales para transmitir la señal de reloj, aunque no es lo más común.
- Lo normal es codificar la señal de reloj para incluirla en la señal de datos.

Código Manchester 1 → L - H 0 → H - L



A mayor velocidad de transferencia mayor probabilidad de que se requiera una transmisión síncrona.

Interfaz DTE-DCE. Normas ITU-T V.24/V.28

La normalización de este interfaz es necesaria para estandarización de la conexión entre equipos informáticos y equipos de comunicaciones. Se normaliza para tener compatibilidad con otros equipos de otros fabricantes.

Este interfaz es equivalente a RS-232-D

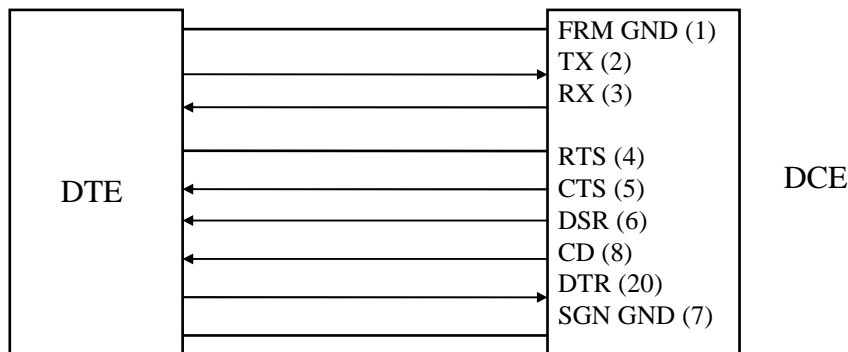
La norma V.24 define las especificaciones funcionales, es decir, las señales que debe haber y las secuencias que deben seguirse para activarlas.

La norma V.28 regula las especificaciones eléctricas y mecánicas. Especificaciones eléctricas:

- Hay que usar señales binarias sin balancear.
- El voltaje en circuito abierto debe ser menor de 25 voltios.
- El voltaje de uso está comprendido entre 5 y 15 voltios positivo y negativo.
- La corriente en cortocircuito debe ser menor que 0.5 A.

En cuanto a las especificaciones mecánicas, la norma especifica un conector DB-25 o DB-9.

Con estas características eléctricas se consiguen velocidades de hasta 20Kbps para 15 metros de cable. En función del tipo de cable y la distancia se podrán obtener velocidades mayores. En cuanto a las características funcionales (V.24), la norma contempla 21 señales pero de ellas las más utilizadas son sólo 9



FRM GND: masa de protección

SGN GND: Signal Ground, línea de retorno común que cierra todos estos circuitos.

DTR (108): Data Terminal Ready, indica que el terminal de datos está conectado.

DSR (107): Data Set Ready, indica que el modem está conectado.

CD (109): Carrier Detect, indica que detecta portadora, es decir, que el DCE se ha comunicado con el DCE remoto.

RTS (105): Request To Send, solicitud de transmisión.

CTS (106): Clear To Send, indica que el DCE está listo para recibir datos.

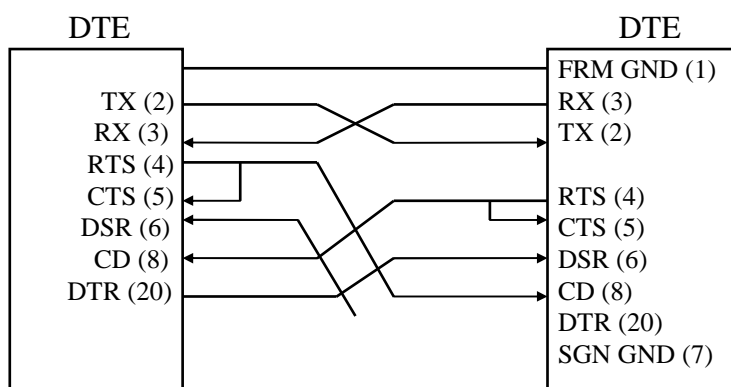
Protocolo a seguir:

1. DTE A $\xrightarrow{\text{DTR}}$ DCE A
 $\xleftarrow{\text{DSR}}$
2. DTE A $\xrightarrow{\text{RTS}}$ DCE A
3. DCE A coloca portadora en la línea
 DCE B detecta portadora
 $\xrightarrow{\text{CD}}$ DCE A
- DTE A $\xleftarrow{\text{CTS}}$ DCE A
4. DTE A $\xrightarrow{\text{Tx}}$ DCE A DCE B $\xrightarrow{\text{Rx}}$ DCE A

La norma V.24 también prevé la existencia de

- una señal TC (Transmisión Clock)
- una señal RC (Recepción Clock)

Se puede utilizar lo que se llama null-modem cruzando las líneas adecuadamente y conectar dos PC's mediante cable serie.



Otras normas:

EIA RS-422 (V.11)

EIA RS-433 (V.10)

No utilizan una línea de retorno común

La primera utiliza transmisión balanceada (mejores prestaciones), mientras que la segunda utiliza transmisión no balanceada.

Se alcanzan distancias de hasta 1200 metros y con la primera velocidades de hasta 10Mbps y con la otra de hasta 100Kbps.

La ITV-T V.35 utiliza también transmisión balanceada y se utiliza en líneas de como mínimo 64Kbps. Tiene 3 líneas de pins y 34 patillas.

Interfaz DCE local - DCE remoto

Estas normas también especifican el modo de modulación.

V.22 especifica transmisión duplex a 1200 bps y modulación PSK

V.22 bis especifica transmisión duplex a 2400 bps y modulación PSK

V.32 especifica transmisión duplex a 9600 bps y modulación PSK

V.32 bis especifica transmisión duplex a 14400 bps y modulación PSK

V.32 terbo especifica transmisión duplex a 19200 bps y modulación PSK

V.34 especifica transmisión duplex a 28800 bps y modulación PSK

Las mejoras de estas normas se basan en tratar de minimizar el tiempo de establecimiento de las conexiones.

Norma que regula el uso de fax en modems: V.29

Multiplexación

Como el cableado es lo más costoso, se tienden cables que permitan muchas comunicaciones.

Un canal se comparte entre varios usuarios de varias maneras:

- asignar a cada usuario un rango de frecuencias distintas.
- asignar un periodo de tiempo a cada usuario.

Estas formas dan lugar a dos formas de multiplexación:

- Multiplexación en frecuencia (FDM), técnica de transmisión analógica de banda ancha en la cual se transmiten simultáneamente múltiples señales sobre un único conductor físico. Se modulan las señales con portadoras de distintas frecuencias.
- Multiplexación por división en el tiempo (TDM), es una tecnología de banda base en la cual se identifican los circuitos individuales por su posición en un flujo de tramas que tienen intervalos regulares de tiempo asignados. A cada usuario se le asigna un quantum de tiempo de manera que en cada instante solo se transmiten los datos de un usuario.

TDM en principio sería más adecuada para transmitir datos, aunque hoy en día se utiliza para transmitir voz.

Una variante de la multiplexación por división en el tiempo es la multiplexación estadística, en la cual se asignan los quantums de tiempo en función del uso anterior de ese canal. Estos circuitos son más caros que los anteriores.

Conmutación

Es el proceso mediante el cual se pone en comunicación un usuario con otro a través de una infraestructura común para la transferencia de información.

La conmutación se lleva a cabo de varias formas:

1º) Conmutación de circuitos: consiste en el establecimiento previo al envío de información de un camino físico entre emisor y receptor, que se mantiene abierto durante todo el tiempo que dura la transferencia de información.

Para establecer el camino físico se usan dos técnicas de señalización distintas:

- *señalización por canal asociado:* por el mismo canal por el que se realiza la transferencia de datos.
- *señalización por canal común:* la infraestructura común comparte un canal que sirve para el establecimiento de los circuitos.

La conmutación de circuitos es la más adecuada para la voz.

Ventajas: una vez que se ha establecido el camino, toda la información irá por el mismo canal físico. No hay peligro de congestión de la infraestructura común de comunicaciones. La información llega a su destino en el mismo orden en el que sale.

Desventaja: el hecho de tener que establecer un camino previo a la transmisión, introduce un retardo.

2º) Conmutación de mensajes: es un método basado en el tratamiento de bloques de información. Cada bloque de información está dotado de dirección de origen y dirección de destino. No se requiere el establecimiento de un camino previo a la transferencia de información.

Ventaja: no se requiere el establecimiento de un camino previo.

Desventajas: cada mensaje lleva dirección de origen y destino. Los elementos de la red deben tener capacidad para almacenar mensajes. Posibilidad de congestión de la red.

A partir de la conmutación de mensajes surge la conmutación de paquetes, que sigue el mismo principio pero establece una longitud fija para el tamaño de los paquetes. Con esto se consigue que el espacio de almacenamiento en los nodos intermedios sea menor.

Ventajas: las mismas que la conmutación de mensajes.

Con este tipo de conmutación no se garantiza que se reciban los mensajes en el mismo orden en que fueron emitidos. Adecuado para transmitir datos.

Diferencias entre conmutación de circuitos y de paquetes:

Conmutación de circuitos	Conmutación de paquetes
Se reserva el ancho de banda al inicio	Se reserva ancho de banda a medida que se necesita
No se puede colapsar un enlace	Tráfico repentino puede colapsar la red
Datos llegan en el mismo orden en que se han originado	Datos pueden llegar en distinto orden
Precio en función de la distancia y del tiempo	Precio en función del tráfico y de la distancia

2.4 Cableado Estructurado

Actualmente se cablea un edificio con un cable estándar, de manera que se apto para las comunicaciones de datos.

Con el nuevo sistema de cableado se persiguen:

- Modularidad, atañe al crecimiento de la red, que sea fácil añadir terminales de datos, cambiarlos de sitio y localizar averías.
- Flexibilidad, hace referencia a la posibilidad de conectar equipos de diferentes fabricantes, distintas LAN's y debe permitir distintas velocidades de transmisión.

Dos estándares que se suelen aplicar: EIA-568 y EIA-569

Estas normas describen la arquitectura, los tipos y la gestión que se hace del tipo de cableado.

El sistema de cableado de un edificio se descompone en 3 subsistemas:

- Subsistema de distribución horizontal, sirve para conectar terminales de una planta (Cableado de planta).
- Subsistema de distribución vertical, conecta las plantas entre sí (Cableado troncal).
- Salas de comunicación, lugares donde se interconectan los subsistemas de cableados.
 - Salas de cableado de planta (FCR)
 - Salas de comunicación de edificio (BCR)

Las LAN's utilizan tres tipos de topología: bus, anillo y estrella.

Los sistemas de cableado de un edificio utilizan una topología de estrella.

Concentradores (HUB, MAU): dentro de ellos se constituye el bus o anillo.

Para el cableado troncal se utiliza indistintamente par trenzado, coaxial o fibra óptica. Para el subsistema de distribución horizontal se suele usar par trenzado de categoría 5.

2.5 RDSI (ISDN)

Se buscaba un sustituto de la red telefónica. El CCITT la definió como una red que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios y al a que los usuarios acceden a través de un conjunto definido de interfaces normalizados.

No será necesario adecuar las señales de los ordenadores para transmitir por este medio.

Principal inconveniente de pasar de la red telefónica básica a la RDSI es la sustitución de infraestructura y del bucle de abonado (par de cobre que va de las centrales al domicilio de los usuarios). Pero la RDSI aprovecha el mismo bucle local que la telefonía básica. Esto ha provocado la expansión de su uso.

La RDSI utiliza la señalización por canal común.

La arquitectura de la RDSI se describe con una serie de equipos y una serie de referencias:

TE1 = terminales digitales (teléfono digital, PC con tarjeta RDSI)

TE2 = terminales analógicos (teléfonos, faxes)

TA = adaptador de terminales, para hacer compatibles equipos analógicos con la red RDSI.

NT2 (RT2) = terminales de red de tipo 2, central de conmutación para conmutar terminales conectados a ella entre sí

NT1 (RT1) = terminal de red de tipo 1, es el elemento que permite el acceso a la red digital.

Clasificación de canales:

A = canales analógicos de voz ,4khz

B = 64 Kbps digital

C = 8 o 16 Kbps digital
D = 16 o 64 Kbps digital
E = 64 Kbps digital
H = 384, 1536, 1920 Kbps

La RDSI emplea canales de tipo B y D. Sólo emplea dos combinaciones:

- acceso básico 2B + 1D (16 Kbps)
- acceso primario 30B + 1D (64 Kbps)

Los canales de tipo B son los que va a utilizar el usuario, los de tipo D se emplean para señalización por canal común y no son accesibles por el usuario.

Los dos canales de tipo B permiten establecer dos circuitos.

¿Cómo comparten el bucle de abonado los diversos canales?

Utilizan la técnica de multiplexación en el tiempo

TEMA 3 EL SUBNIVEL DE ACCESO AL MEDIO

3.1 Introducción

El subnivel de acceso al medio tiene que ver con las redes por canales de difusión. Su función es arbitrar el acceso al canal cuando compiten por él.

Características diferenciadoras de las LAN:

- La transmisión de la información es siempre digital
- Alto grado de conexión de los equipos implicados
- Elementos relativamente económicos
- Alta velocidad de transferencia de la información

- Baja tasa de errores
- Topología de la red, en bus o anillo
- Suelen estar al servicio de una única entidad

¿Cómo repartir el canal entre las múltiples estaciones que se pueden conectar a él?

Básicamente hay dos métodos de asignación de canales:

- **Estáticos** (multiplexación por división en el tiempo o en la frecuencia)
Estos métodos no son apropiados para LAN's ya que hay muchas máquinas compartiendo la red. Además el número de máquinas conectadas es variable. Se buscan métodos que asignen de forma dinámica los canales como la multiplexación estadística.

El modelo de estaciones consta de N estaciones independientes, cada una de ellas genera información a transmitir agrupada en tramas. Asumimos que las estaciones están dedicadas a las comunicaciones (cuando decide enviar una trama, no hace nada más hasta que lo consigue).

Asumiremos que hay un medio único para la transmisión de las tramas, en el cual todas las estaciones vierten sus tramas y todas reciben los datos de él.

Existencia de colisiones: si dos estaciones intentan verter sus datos en el medio a la vez.

Patrones de tiempo:

- *Continuo*, las estaciones pueden verter su información en el medio en cualquier instante.
- *Ranurado*, se usa un reloj maestro que divide el tiempo en intervalos de igual duración, cada intervalo se llama ranura o time-slot. La transmisión de una trama solo se puede hacer coincidiendo con el inicio de un time-slot.

Para cada time-slot se pueden dar tres situaciones:

- No se transmite ninguna trama
- Se transmite una trama (éxito)
- Si se intentan verter en el medio más de una trama → colisión

Detección de portadora: se identificará con la existencia de una trama en el medio.

En cada situación optaremos por un patrón de tiempo y por la detección o no de portadora. Esto supone saber si el canal está ocupado (escuchar el canal), si está ocupado no se verterá la trama en el medio.

Los primeros métodos que se establecieron para controlar el acceso al medio se usaron en paquetes vía radio. Se llaman protocolos ALOHA desarrollados en los años 70 en la universidad de Hawai. El primer protocolo fue ALOHA puro.

Las estaciones son capaces de detectar una colisión. Cuando detecta una colisión se espera un tiempo y vuelve a transmitir los datos.

ALOHA ranurado, divide el tiempo en intervalos discretos al igual que el anterior ranurado. Como los paquetes ocupaban como mucho un time-slot se mejoró la calidad de la comunicación.

3.2 Protocolos de acceso al medio

Mejora de los protocolos ALOHA, introducir la posibilidad de detectar si el canal está siendo ocupado. Este tipo de protocolos se denomina CSMA (Carrier Sense Multiple Access). Dentro de los protocolos CSMA se distinguen 3 tipos:

- **CSMA 1-persistente:** la estación escucha del medio, si está libre transmite y sino sigue escuchando hasta que detectan que queda libre, en el momento en el cual transmiten. No es un protocolo libre de colisión, si más de una estación están preparadas para transmitir, estarán escuchando del medio y cuando este quede libre intentarán transmitir a la vez. Cuando se detecta una colisión, las estaciones dejarán pasar un tiempo aleatorio antes de volver a testear el canal.
- **CSMA no-persistente:** antes de transmitir escuchan del medio, si está libre no transmiten sino que esperan un tiempo aleatorio antes de transmitir la trama. Se evitan colisiones a costa de introducir retardos.
- **CSMA p-persistente:** se divide el tiempo en time-slots, la estación cuando está lista para transmitir escucha del medio, si está libre transmite con una probabilidad p , mientras con una probabilidad $q=1-p$ espera hasta el siguiente slot.

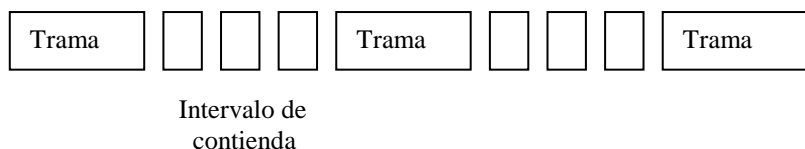
Protocolo CSMA/CD

CD (Collision Detection)

Se abortan las transmisiones que colisionan

Cuando dos estaciones que han transmitido a la vez detectan una colisión, dejan de transmitir. Ahorramos tiempo y ancho de banda.

Este protocolo corresponde con un modelo conceptual como este:



El intervalo de contienda se produce cuando las estaciones intentan hacerse con el dominio del medio.

Es uno de los protocolos más usados (se usan en las LAN ethernet)

Una estación puede tardar en enterarse 2 veces el tiempo de propagación entre las estaciones más alejadas de que se ha producido una colisión.

Un protocolo tiene carácter determinista cuando una estación es capaz de establecer a priori el tiempo máximo que va a tardar en ganar el acceso al medio. En caso contrario será no determinista.

Para redes que conectan robots, no es bueno usar protocolos no deterministas.

Protocolos libres de colisión

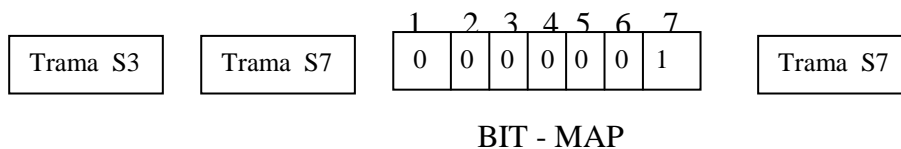
Cuando la carga de la red es baja son mejores los protocolos con colisiones.

- **Método del Bit-Map Básico**

Consiste en establecer unos periodos de contienda que constan de n slots cada uno de ellos (n = número de estaciones). En cada slot solo se puede transmitir un 0 o 1 y en cada uno de esos slots solo puede transmitir una de las estaciones.



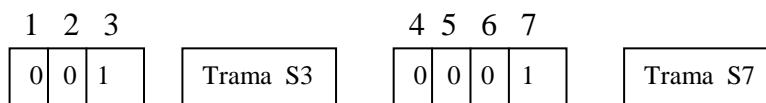
Si la estación tiene tramas para transmitir pone un 1 en su bit correspondiente del mapa de bits. Cuando finaliza el periodo de contienda, ya está establecido el orden de acceso al medio.



Problemas: las estaciones deben esperar al mapa de bits para poder transmitir. El método da preferencia a las estaciones con direcciones bajas.

- **BRAP (Broadcast Recognition with Alternating Priorities)**

Cuando una estación quiere transmitir una trama, espera la llegada del bit map y empieza a transmitir la trama.



- **MLMA (MultiLevel MultiAccess)**

Las estaciones previamente a la transmisión de sus tramas, anuncian su intención de transmitir difundiendo su dirección por la red con un formato dado.

Protocolos de contienda limitada

Combinan las ventajas de los protocolos libres de colisión con los protocolos con colisión. Limitan los intervalos de contienda de manera que si tenemos 1000 estaciones, se agrupan de forma que usando un patrón de tiempo ranurado, durante el primer time-slot solo pueden transmitir las estaciones del grupo 1 y así sucesivamente.

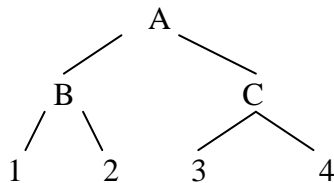
1 ... 100 101 ... 200 201 ... 300

grupo 1 grupo 2 grupo 3

Cuando más estaciones se introduzcan en un grupo habrá más posibilidades de colisión, pero menos retraso.

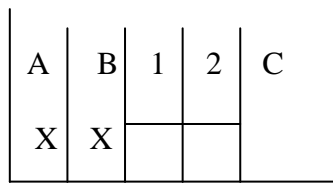
- **Protocolo Adaptativo Tree-Walk**

Es similar a la busca dicotómica en un vector.



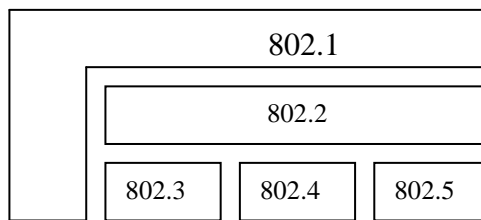
Se divide las estaciones en grupos, A contiene todas las estaciones y a su vez se divide en B y C, hasta conseguir grupos de una sola estación.

Durante el primer time-slot se permite transmitir a todas las estaciones del grupo A, en situaciones de mucha carga se producirán colisiones.



3.3 Estándares IEEE 802 para redes de área local

Vamos a ver implementaciones reales de lo que vimos en el tema anterior. Podemos resumir el conjunto de normas 802 con el siguiente esquema:

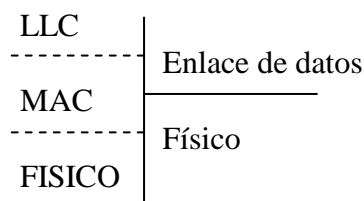


Se ha empezado a trabajar con normas de este estilo a mayores velocidades de transmisión.

802.1 uso de primitivas y normas con lo que van a trabajar las demás

802.2 corresponde al nivel de enlace de datos en el modelo OSI. Se llama LLC (Logic Link Control)

Podemos hacer unas equivalencias entre el modelo OSI y las normas IEEE 802



IEEE 802.3 y Ethernet

Aunque se suelen confundir y se suele hablar indistintamente, Ethernet y 802.3 no son equivalentes. Ethernet se desarrolló inicialmente como una tecnología de banda ancha. Otras aproximaciones optaron por la transmisión digital. La unión de todas las tecnologías que surgieron utilizando el protocolo CSMA/CD dio lugar a las normas 802.3

Intel y Xerox sentaron las bases de estas normas. Aunque la norma cubre el nivel de acceso al medio y el nivel físico, en cada norma distinguiremos estos dos niveles.

	10 BASE 5	10 BASE 2	1 BASE 5	10 BASE T	10 BROAD 36
Velocidad Trans.	10	10	1	10	10
Long. Max. Segm.	500	185	250	100	1800
Medio físico	Coaxial grues	Coaxial fino	UTP	UTP	Coax. CATV
Topología	BUS	BUS	ESTRELLA	ESTRELLA	BUS

Significado del nombre: 10 BASE T

- 10 → velocidad de transferencia, en Mbps
- Base → indica el modo de transmisión, banda base o banda ancha (broad)
- T → hace referencia al medio físico de transmisión. En principio trata de indicar la longitud máxima del segmento.
 - F indica que el medio físico es fibra óptica
 - T cable de par trenzado

Coaxial CATV = cable coaxial de TV, cuya impedancia es de 75Ω

Aquí aunque todas las estaciones estén unidas al mismo bus, lo que representa el medio es la topología del cableado por eso aparece topología ESTRELLA.

Los conectores pueden ser de dos tipos:

- Cable coaxial BNC
- Cable de par trenzado RJ-45

Es posible ver tarjetas de PC con ambos tipos de conectores. La forma de conectar estos conectores es mediante un dispositivo en forma de T. Los conectores para el cable coaxial grueso son de otro tipo.

El cable debe estar cerrado por ambos extremos con una resistencia de 50Ω (en circuito abierto no funciona)

La forma más sencilla de montar una red es utilizando concentradores o Hubs

Para migrar de una red 10 Base T a 100 Base T sería necesario:

- Cambiar placas
- Cambiar concentradores

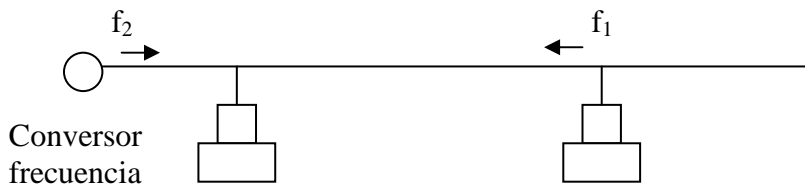
En el caso de 10 Broad 36, no cuadra la longitud del segmento (1800) con lo que se ha explicado antes.

En banda base:



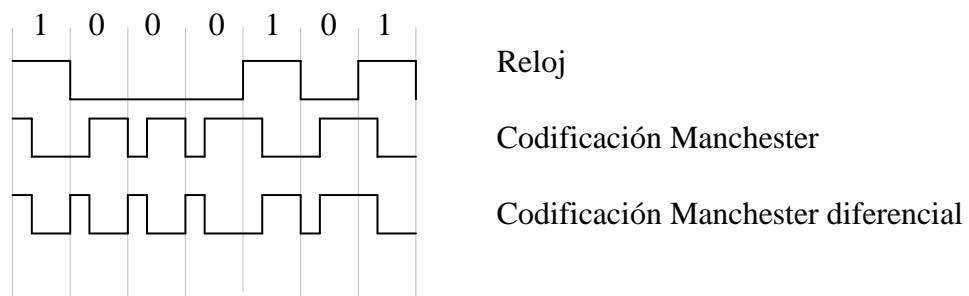
La información se difunde a ambas partes simultáneamente.

En banda ancha esto no es posible, la señal se propaga en un sentido que se hacia la cabecera de la red y la cabecera actúa como convertor de frecuencias de manera que todas las estaciones emiten con frecuencia f_1 y reciben con una frecuencia f_2



De sumar estas frecuencias se obtiene el valor anterior. La ventaja está en la distancia máxima del segmento que aquí es mayor.

Codificación Manchester



La codificación Manchester se caracteriza porque siempre a mitad de tiempo de bit se produce una transición:

De 0 a 1 → para ceros

De 1 a 0 → para unos

Esta señal lleva implícita la señal de reloj

Código Manchester diferencial

Se caracteriza porque los ceros además de presentar una transición a mitad del tiempo de bit, también la presentan al inicio del tiempo de bit.

Características de la norma en su nivel de acceso al medio

Trama, es la estructura de codificación de un flujo de bits a través de un enlace.

Formato de la trama 802.3

7	1	2 o 6	2 o 6	2	0 – 1500	0 – 46	4
Preámbulo	STF	DA	SA	Long.	DATOS	PAD	CS

nº superior = octetos de los que consta cada campo de la trama

Preámbulo: parte de la trama que sirve para la sincronización de la estación receptora.

STF (Start Of Frame): inicio de trama

DA (Desting Address): dirección de destino

SA (Source Address): dirección de origen

En principio se puso definir dos tipos de direcciones:

- locales, se podrán configurar
- globales, únicas. Si se debe reservar una dirección única para cada estación de red, se necesita más espacio (de ahí los 6 octetos).

El formato de las direcciones es:

bit 47bit 0

Si bit 47 = 0 dirección individual

Bit 47 = 1 dirección de grupo (enviar una trama a un conjunto de estaciones)

La mayoría de algoritmos de red utilizan direcciones globales e individuales.

LONG: indica lo largo que va a ser el campo de datos. Con 1 octeto no sería suficiente, solo nos indicaría 255 datos.

PAD: campo de relleno. Se hace uso de éste solo si la longitud de la trama es menor de 64 octetos, ya que para distinguir una trama de basura es necesario que estas sean al menos de 64 bytes.

CS (Check Sum): campo de comprobación de la integridad de la trama, 32 bits de comprobación.

¿Qué ocurre cuando se produce una colisión?

Protocolo CSMA/CD no era libre de colisiones.

Nada más detectarlo las estaciones abortan la transmisión de sus tramas y además envían una señal para avisar. Después esperan un tiempo aleatorio antes de empezar a transmitir.

El tiempo se divide en intervalos discretos, que vienen dados por el mayor retardo de propagación de la red, de manera que si se produce una nueva colisión detectarlo.

Después de la primera colisión cada estación espera un time-slot antes de empezar a transmitir.

Tras i -colisiones consecutivas, cada estación después de la colisión i -ésima espera un número que va de 0 a 2^{i-1} time-slots.

Esto tiene un límite, cuando se llega a las 10 colisiones el intervalo será de 1023 y tras 16 colisiones se “tira la toalla”, error y no se puede volver a transmitir.

IEEE 802.4 TOKEN-BUS

En una red no determinista es imposible predecir en cuanto tiempo accederá un servidor a la red, esto es crítico para líneas de producción como General Motors.

Se estableció una serie de turnos para acceder a la red, cada estación tiene su turno para transmitir, con esto garantizamos que podremos conocer el tiempo en que tardará una estación en transmitir.

Otra cosa que no gustaba de la red IEEE 802.3 era que no se podían establecer prioridades. En esta red cada trama tiene una prioridad. Los técnicos de General Motors no eran partidarios de una red en anillo.

Los turnos se establecen haciendo circular un testigo, en cada instante solo puede transmitir la estación que tiene el testigo.

- **Nivel físico:** se usa cable coaxial de 75Ω , variantes de la modulación FSK, las velocidades de transferencia van de 1,5 a 10 Mbps.
- **Nivel MAC (acceso al medio):** se establecen 4 niveles de prioridad distintos y se subdivide cada estación en 4 partes como si tuviéramos 4 subestaciones, esto hace que las tramas se encolen en la cola correspondiente a su prioridad. Todas las estaciones empiezan a transmitir por la cola más prioritaria.

Formato de la trama:

P	SD	FC	DA	SA	DATOS	CS	ED
1	1	1	2 o 6	2 o 6	0 – 8182	4	1

P: preámbulo

SD: delimitador de inicio de trama

FC: (Frame Control), delimita si es una trama de datos o de control

DA, SA: direcciones de inicio y destino

CS: Check Sum

ED: delimitador de final de trama

No hay un campo de longitud para saber la longitud de la trama, ya que posee un delimitador de fin de trama. Sólo tiene un octeto de preámbulo ya que no existen colisiones a diferencia de los 7 octetos de preámbulo del IEEE 802.3, que se usan para detectar colisiones.

En este formato hay más octetos de datos ya que no se pierde tiempo de contienda y el tiempo de transmisión está limitado por un temporizador.

IEEE 802.5 TOKEN-RING

Desarrollado por IBM para sus redes de área local. Se estructura como un anillo físico al que se conectan todas las estaciones. Por ese anillo físico se hace circular un testigo siempre en el mismo sentido, una estación sólo puede transmitir si tiene el testigo. Las estaciones transmitirán en el orden en que están conectadas al anillo.

Las estaciones que vierten las tramas al anillo también las retiran, de manera que las tramas siempre dan la vuelta completa al anillo.

- **Nivel físico:** se suele utilizar cable de par trenzado apantallado, se consiguen velocidades de transferencia 4/16 Mbps.

El anillo se construye dentro del Wir-Center o MAU, con esto disminuye el peligro de que se corte el anillo.

Para la transmisión utiliza codificación diferencial Manchester

Niveles eléctricos 0 = [+3, +4'5] 1 = [-3, -4'5]

- **Subnivel MAC:** se tiene dos tipos de tramas (testigos y datos)

1	1	1
SD	AC	ED

Testigo

SD: starting delimiter

AC: access control

ED: delimitador de final de trama

	1	1	1	2 o 6	2 o 6	sin limite	4	1	1
Datos	SD	AC	FC	DA	SA	DATOS	CS	ED	FS

El SD y ED tienen unos bits especiales

SD JK0JK000

ED JK1JK1IE

que en ningún caso se van a poder dar dentro del campo de datos. Violación de la codificación del nivel físico, con esto se asegura que se distinguirá que octeto empieza y que octeto finaliza la trama.

- **Campo AC** (Access Control)

Formato: PPPTMRRR

PPP indica la prioridad del token o de la trama

Las estaciones para poder transmitir deben capturar un testigo que tenga una prioridad igual o menor que la de las tramas que va a transmitir.

RRR reserva de prioridad

Cuando a una estación le llega el testigo con una prioridad con la que no puede transmitir indicará en la reserva de prioridad, la prioridad de sus tramas siempre y cuando la reserva de prioridad del testigo que le ha llegado sea menor que la que va a reservar.

bit T si 0 token
si 1 trama

bit M (monitor) sirve para evitar que un token prioritario esté circulando siempre por el anillo. Una estación del anillo es el monitor activo, cuando ve pasar un token prioritario pone M a 1 y cuando vuelve a verlo pasar le baja la prioridad.

- **Campo FC** (Frame Control)

Su contenido es distinto si la trama es de datos, en cuyo caso la genera un nivel superior y no es significativo a nivel de acceso al medio) o si la trama es de control.

- **Campo FS** (Frame Status)

Formato AACC

bit A de dirección reconocida

bit C de trama copiada

Cuando una trama se vierte al anillo inicialmente A y C están a cero. Cuando una estación reconoce la dirección pone A a 1 y además debe copiar la trama en su buffer en cuyo caso pone C a 1. Cuando la trama vuelve a la estación de origen si tiene los cuatro bits a 1 le indica que la trama se ha reconocido con éxito.

<u>A</u>	<u>A</u>	<u>C</u>	<u>C</u>
0	0	0	0
0	0	1	1

dirección no reconocida y por tanto no copiada

imposible

1 1 0 0 se ha reconocido la trama pero no se ha copiado

Todas las estaciones conectadas a una red token-ring funcionan en dos modos:

- Modo operacional
- Modo monitor: todas las estaciones menos una serán monitor pasivo y esa otra estará en modo monitor activo. Esta estación debe preocuparse de que siempre haya un testigo circulando por el anillo. Esto funciona a través de temporizadores.

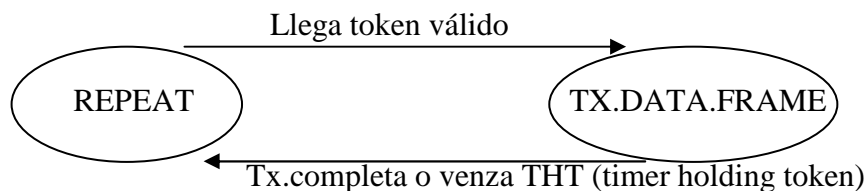
Tramas MAC

- **Claim Token:** sirven para reclamar el testigo, para que las estaciones traten de erigirse en monitor activo. Cuando una estación determina que no hay monitor activo entra en estado de reclamación de token y transmiten tramas de este tipo.
- **Duplicate Address Test (DAT):** esta trama la mandan cuando se conectan las estaciones al anillo para comprobar que la dirección con la que van a conectarse es única. En esta trama se indica la dirección de la estación como dirección destino, si cuando vuelve la trama ninguna estación ha reconocido la trama su dirección es única.
- **Active Monitor Present (AMP):** la estación con monitor activo manda estas tramas para indicar a las demás que existe una estación con monitor activo.
- **Purge (PRG):** tramas de inicialización del anillo. Las genera el monitor activo después de una pugna por la transmisión del token.

Formas de representar protocolos:

1. Máquina de estados finitos
2. Lenguaje algorítmico

Funcionamiento en modo operacional



Funcionamiento modo monitor

Partimos de un estado BYPASS en el cual la estación todavía no está insertada en el anillo. Cuando se conecta, lo primero que hace es enviar una trama DAT, si le llega devuelta con el bit de dirección reconocida A=1, la estación debe desconectarse. En caso contrario A=0, se pasa a un estado STANDBY estado en el que normalmente está la estación en modo pasivo. Si estando en este estado se produce un error o la estación se desconecta pasa a estado BYPASS. Si durante un cierto tiempo no recibe tramas AMP o no le llega el testigo, pasa al estado de reclamación del testigo y transmite tramas CL_TK si le llega la misma trama enviada pasa a modo activo, en caso contrario pasa a modo STANDBY.

3.4 Redes de fibra óptica: FDDI

Ideas que sugirieron su creación:

- Incrementar la velocidad
- Mayor fiabilidad, consta de 2 anillos

Esta norma se recogió en IEEE 802.8

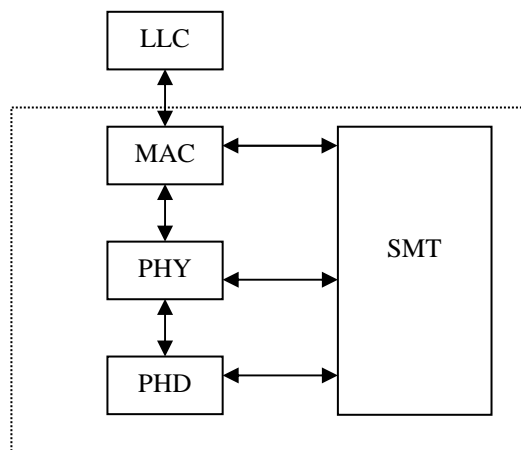
La utilización de FDDI es para LAN'S de muy alta velocidad o como red "backbone" para conectar otras redes.

Especificaciones del nivel físico:

- Velocidades de transferencia de 100 Mbps
- Acceso al medio mediante pase de testigo
- Anillo dual
- Fibra óptica

Se pueden conectar hasta 1000 estaciones con una separación entre ellas máxima de 2 kilómetros. La longitud total de la red puede ser de 200 km. Tiene todas las ventajas de la fibra óptica.

La norma consta de cuatro especificaciones separadas:



MAC: se describe el protocolo de acceso al medio, la estructura de la trama (igual a 802.5) mecanismos de manejo del token, algoritmos cálculo check-sum, detección de errores.

Se utiliza codificación 4B/5B: agrupar los bits del usuario de 4 en 4 y asignarle a cada combinación un valor de 5 bits.

<u>Datos</u>	<u>Código</u>
0000	11110
0001	01001
.....
1111	11101

También se utiliza violación del nivel físico para delimitar las tramas.

Anillo dual con tráfico en direcciones opuestas. Al anillo primario se conectan la mayoría de las estaciones de forma similar a la red token-ring y el anillo secundario se usa como backup en caso de que falle el primario.

Dependiendo de si se conecta a uno o a los dos anillos tenemos varios tipos de estaciones:

- estaciones que solo se conectan al anillo primario, clase B (SAS) Single AS
- estaciones que se conectan a los dos anillos, clase A (DAS) Dual Attached Station

La fiabilidad de estas redes la garantizan las estaciones DAS.

Si se produce un fallo en una estación, el subnivel MAC lo detectará y será capaz de doblar el anillo, al igual que se falla un segmento de fibra. Las estaciones DAS suelen ser concentradores.

TEMA 4 EL NIVEL DE ENLACE DE DATOS

4.1 Introducción

El nivel de enlace de datos se encarga de conseguir una conexión fiable y eficiente entre dos máquinas como si estuvieran conectadas conceptualmente por un cable.

Debe ser capaz de proporcionar a la máquina destinataria, la secuencia de bits que ha originado la máquina emisora, en el mismo orden.

Funciones del nivel de enlace de datos:

- prestar servicios al nivel superior (función general de todos los niveles)
- agrupar la información en tramas
- control y recuperación de errores
- control del flujo de información entre dos estaciones, es necesario ya que todas las estaciones no son iguales y cada una puede transmitir a una velocidad.
- gestión y administración del enlace de datos.

Delimitación de tramas

1º) Conteo de caracteres: incluir un campo en la trama que indica el número de octetos que la componen.

2º) Caracteres de inicio y final con “stuffing” de caracteres: cada trama se inicia con la secuencia de dos caracteres ASCII (DLE + STX) y para terminar se usa (DLE + ETX).

Para evitar que se confunda estos caracteres con los datos de la trama, el nivel de enlace de datos de la máquina emisora cuando detecta en los datos a enviar el carácter DLE, lo duplica. Y el receptor cuando detecte dos DLE seguidos eliminará uno.

Datos: A DLE ETX B DLE STX
 Trama a enviar: DLE STX A DLE DLE ETX B DLE DLE STX DLE ETX
 Trama recibida: A DLE ETX B DLE STX

3º) Flags de inicio y final con bit-stuffing

Cada trama se inicia y finaliza con una secuencia 0111111001111110

Para no confundir con los datos se añade, cuando se detectan cinco unos seguidos, un cero.

Materializa un cero y sigue con los datos, con esto se evita que se confundan los datos con el flag del final.

4º) Violación de codificación del nivel físico, utiliza una codificación distinta que la de los datos para los flags de inicio y fin de trama.

Todos los métodos introducen una sobrecarga y en el caso 2 y 3 esta sobrecarga es variable dependiendo de los datos que se transmitan.

4.2 Detección y Corrección de errores

Los errores se pueden producir por muchas causas. En transmisión de datos picos que pueden ser insignificantes en otro tipo de transmisiones, son muy perjudiciales.

Un pequeño ruido provoca que se estropeen muchos bits. Para detectar y corregir los errores se debe introducir información redundante a la que se transmite. Se puede introducir información redundante para que el receptor detecte el error (detección) o introducir más información redundante para que el receptor pueda corregir el error (corrección).

$$\begin{array}{ll}
 d_0 \dots d_m \ c_1 \dots c_r & d = \text{bits de datos que proporciona el nivel de red} \\
 n = m + r & c = \text{bits de redundancia}
 \end{array}$$

Palabra código es la suma de estos bits.

La distancia de Hamming entre palabras código es el número de posiciones individuales de bit, que difieren entre las dos palabras código.

Ejemplo:

$$\begin{array}{r}
 00100101 \\
 \underline{01000101} \\
 01100000
 \end{array}
 \qquad \text{distancia Hamming} = 2$$

Dos palabras código que difieran una distancia Hamming x, requerirán x errores individuales de bit para convertirse la una en la otra.

La detección de errores se basa en el principio de que en una transmisión no todas las combinaciones de los n bits son válidas, aunque si son válidas cualquier combinación de los m bits de datos.

La distancia de Hamming de un código completo, es la mínima distancia de Hamming entre dos palabras código válidas.

Método de detección de errores (Paridad)

Cuenta el número de unos que hay en los datos. La paridad puede ser par (se añade el bit de paridad para que haya un número par de unos) o impar (se añade el bit de paridad para que haya un número impar de unos).

<i>Ejemplo:</i>	$m = 4$	Paridad par	0 0 0 0	0	valida
	$r = 1$		0 0 0 0	1	X
			0 0 0 1	0	X
			0 0 1 0	0	X
			0 0 1 0	1	valida

Este método solo puede detectar un error de bit.

Para detectar d errores individuales de bit, será necesario un código con una distancia de Hamming $d+1$

Corrección de errores

0 0 0 0 0	0 0 0 0 0	mínima distancia de Hamming = 5
0 0 0 0 0	1 1 1 1 1	
1 1 1 1 1	0 0 0 0 0	
1 1 1 1 1	1 1 1 1 1	

Se manda 1 1 1 1 1 0 0 0 0 0, y se recibe 1 0 1 1 1 0 1 0 0 0

La distancia de Hamming entre lo recibido y lo enviado es 2. El receptor reconstruye lo recibido acercándolo a la palabra válida más cercana.

Para corregir d errores, es necesario un código con una distancia de Hamming $2d+1$

Construcción de un código para la corrección de errores de un bit

$$d_1 \dots d_m \quad c_1 \dots c_r \quad n = m + r$$

Por cada mensaje legal $\rightarrow (n+1)$ combinaciones

Combinaciones posibles $2^n \geq 2^m (n+1) \Rightarrow$ $m + r + 1 \leq 2^r$ Regla de Hamming

La Regla de Hamming indica los bits de redundancia necesarios para corregir errores en palabras de m bits

Para palabras de 4 bits \rightarrow serán necesarios 3 bits de redundancia

Para palabras de 11 bits \rightarrow serán necesarios 4 bits de redundancia

El código que cumple la igualdad en la regla de Hamming, se denomina código óptimo.

Método de corrección de errores de Hamming

Se basa en dado un vector palabra código $c = (c_1, c_2, \dots, c_n)$ y un vector de datos $d = (d_1, d_2, \dots, d_m)$, hacer que se cumpla la igualdad $d \times G = c$, donde G es una matriz generadora de paridad $G = [I : A]$

Ejemplo:

$m = 4$	1 0 0 0	1 1 1
$r = 3$	0 1 0 0	0 1 1

$$G = \begin{array}{cccccc} 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array} \quad \begin{array}{l} d = [1 \ 0 \ 1 \ 0] \\ d \times G = [1 \ 0 \ 1 \ 0 \mid 0 \ 1 \ 0] \end{array}$$

La operación se realiza en aritmética módulo 2 (la multiplicación como AND bit a bit y la suma como XOR). *Ejemplo:*

$$\begin{array}{r} 1 \ 0 \ 1 \ 0 \\ \text{AND } 1 \ 0 \ 0 \ 0 \\ \text{XOR } (1 \ 0 \ 0 \ 0) = 1 \end{array}$$

En la recepción se utiliza una matriz $H = [A^T : I]$. Se tiene un vector de comprobación de paridad $s = (s_1, s_2, \dots, s_n)$ que se obtiene de $s = H r$

Si en la transmisión no se ha producido ningún error entonces $r = c$

Ejemplo:

$$S = \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \times \begin{array}{c} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ r \end{array} = \begin{array}{c} 0 \\ 0 \\ 0 \end{array}$$

H

Cuando s da todo ceros, se interpretará como que la recepción ha sido correcta. Este es el caso en que $c = r$

Suponemos ahora que $c \neq r$

$$S = \begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \times \begin{array}{c} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ r \end{array} = \begin{array}{c} 1 \\ 1 \\ 1 \end{array}$$

H

Para corregir el error se comprueba el vector s , con que columna de la matriz H coincide y esto indica el número de bit que se ha cambiado.

Como los errores no se producen saltados sino a ráfagas, la transmisión se realiza en bloques para permitir corregir ráfagas de errores de hasta 4 bits (en este caso):

$$\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & c & c & c \\ 1 & 0 & 1 & 0 & c & c & c \\ 1 & 1 & 1 & 1 & c & c & c \\ 1 & 0 & 0 & 1 & c & c & c \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & & & \end{array}$$

Método de la comprobación de la redundancia cíclica

Está basado en asimilar las secuencias de bit con polinomios de coeficientes 0 o 1

$$0110110 \Rightarrow 0x^6 + 1x^5 + 1x^4 + 0x^3 + 1x^2 + 1x + 0 \Rightarrow x^5 + x^4 + x^2 + x$$

Para usar este método emisor y receptor acuerdan utilizar un polinomio $G(x)$, que es el polinomio generador. La información redundante generada por este polinomio se denomina checksum.

El cálculo del checksum se lleva a cabo de forma que el polinomio que representa la trama de datos + checksum sea divisible por $G(x)$

$M(x)$ = polinomio que representa los bits de datos

$T(x)$ = trama de datos + checksum

Algoritmo para el cálculo del checksum:

1º) Añadir r bits 0 al final de los datos $x^r M(x)$ $r = \text{grado}(G(x))$

Ejemplo: $G(x) = x^5 + x^4 + x^2 + 1$ $r = 5$
 $M(x) = x^9 + x^7 + x^3 + x^2 + 1 \Rightarrow 101000110100000$

2º) Dividir $x^r M(x)$ entre $G(x)$ utilizando aritmética en módulo 2

$$\begin{array}{r}
 101000110100000 \quad \underline{110101} \\
 \underline{110101} \qquad \qquad 1101010110 \\
 0111011 \\
 \underline{110101} \\
 00111010 \\
 \underline{110101} \\
 00111110 \\
 \underline{110101} \\
 00101100 \qquad \text{cociente } Q(x) \text{ y resto } R(x) \\
 \underline{110101} \\
 0110010 \\
 \underline{110101} \\
 0001110
 \end{array}$$

3º) Restar $x^r M(x) - R(x) = T(x)$ que es lo que se transmite

$$\begin{array}{r}
 101000110100000 \\
 \underline{1110} \\
 101000110101110
 \end{array}$$

4º) Receptor: $T'(x) / G(x) \Rightarrow R'(x)$

Si $R'(x) = 0$ la trama de datos recibida se da como buena

Si $R'(x) \neq 0$ la trama de datos tendrá errores

Aunque si $R'(x) = 0$ no se puede asegurar que no tenga errores ya que pueden haberse producido muchos errores en $T(x)$ y que al dividirlo por $G(x)$ de 0

Condiciones que debe cumplir $G(x)$ para detectar errores de 1 bit:

$$T'(x) / G(x) = T(x) + E(x) / G(x) = T(x) / G(x) + E(x) / G(x)$$

Si solo se ha producido un error en la transmisión: $E(x) = x^i$ $i =$ posición del error

Para detectar errores de un bit, $G(x)$ deberá tener más de un término.

¿Qué debe cumplir $G(x)$ para detectar un número impar de errores?

Si $E(x)$ tiene un número impar de términos, no tiene $(x+1)$ como factor entonces, si $G(x)$ tiene a $(x+1)$ como factor, $E(x)$ no es divisible por $G(x)$

Polinomios más utilizados:

$$\text{CRC-12} \quad G(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$$

$$\text{CRC-16} \quad G(x) = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC-CCITT} \quad G(x) = x^{16} + x^{12} + x^5 + 1$$

Los polinomios de grado 16 son capaces de detectar ráfagas de error de hasta 16 bits.

4.3 Protocolos de enlace de datos

Los niveles físico, de enlace y de red son tres entidades independientes que se comunican a través de unidades de información (mensajes).

El nivel de enlace va a considerar los datos que recibe del nivel de red como sólo datos. Supondremos que el cálculo del checksum lo realiza alguna función y no los protocolos.

Todos los protocolos van a ser guiados por eventos, esto se representará con: esperar (suceso)

Consideremos que las tramas se componen de cuatro campos principales:

- *clase*: indicará el tipo de trama
- *sec*: indicará el número de secuencia (identificador de la trama dentro de un conjunto de tramas)
- *rec*: campo de reconocimiento, esta información la envía la receptora a la máquina emisora informando si se ha recibido correctamente.
- *info*: datos recibidos o a pasar al nivel superior.

Protocolo Simplex sin restricciones

Consideraciones a tener en cuenta:

- Los datos se transmiten en un solo sentido.
- El nivel de red tanto del emisor como del receptor va a estar siempre preparado para enviar y recibir datos.
- El tiempo de proceso es despreciable.
- No hay limitaciones en la capacidad de almacenamiento.
- El canal nunca pierde o daña tramas.
- El único evento posible es la llegada de una trama.

Explicaremos los protocolos con un lenguaje pseudoalgorítmico.

PROTOCOLO 1

tipo SucesosPosibles=(LlegaTrama)

proceso emisor;

var s: trama;
b: paquete;

inicio

repetir

De_N3(b);

s.info:=b;

A_N1(s);

hasta siempre;

fin; (* proceso emisor *)

proceso receptor;

var r: trama;
suceso: SucesosPosibles;

inicio

repetir

esperar(suceso);

De_N1(r);

A_N3(r.info);

hasta siempre;

fin; (* proceso receptor *)

Al aproximarlos a la realidad, surge un problema, ya que el tiempo de proceso no es despreciable y la capacidad de almacenamiento no es ilimitada, tal y como se había considerado en este protocolo.

Protocolo Simplex stop-and-wait

Se tienen en cuenta las mismas consideraciones que en el protocolo anterior excepto que el tiempo de proceso aquí no es despreciable y que la capacidad de almacenamiento no es ilimitada.

Para evitar que se sobrescriban los buffers de entrada en el receptor, si se mandan las tramas muy rápidas, se pueden realizar varias modificaciones, aunque la solución normalmente aceptada es que el receptor comunique al emisor, mediante el envío de una trama, que ya ha procesado la trama anterior y que ya puede enviar la siguiente, esta autorización se conoce como reconocimiento.

PROTOCOLO 2

tipo SucesosPosibles=(LlegaTrama)

proceso emisor;

var s: trama;
b: paquete;
suceso: SucesosPosibles;

inicio

repetir

```

        De_N3(b);
        s.info:=b;
        A_N1(s);
        esperar(suceso);
    hasta siempre;
fin;    (* proceso emisor *)

proceso receptor;
var    r,t: trama;
        suceso: SucesosPosibles;
inicio
    repetir
        esperar(suceso);
        De_N1(r);
        A_N3(r.info);
        A_N1(t);
    hasta siempre;
fin;    (* proceso receptor *)

```

Aunque fluya información en ambos sentidos, para el usuario solamente se transfieren datos en un sentido, con lo que se denomina SIMPLEX. A nivel físico si se deberá utilizar una comunicación semi-duplex, ya que se produce intercambio de información en ambos sentidos.

Protocolo Simplex para un canal con ruido

En este caso se elimina la consideración de que el canal es perfecto y no pierde o daña tramas.

El receptor solo enviará una trama de reconocimiento si le llega la información en buen estado, sin ningún error.

En caso de producirse un error, éste se recupera de la siguiente manera: se asocia al emisor un temporizador de forma que con la transmisión de una trama se inicializa el temporizador, cuando vence éste, sino se ha recibido la trama de reconocimiento, el emisor interpretará que se ha producido un error en la transmisión y volverá a enviar la trama de datos.

Con esto se corrige la pérdida de las tramas de datos, pero si se pierde la trama de reconocimiento, el emisor volvería a enviar la trama de datos y en la recepción se tendría un duplicado de los datos.

El problema de la duplicación de tramas se resuelve asignando un identificador a cada trama. Como solo es necesario distinguir una trama de la anterior, con un bit de identificación será suficiente.

PROTOCOLO 3

```

const MaxSeq=1
tipo  SucesosPosibles=(LlegaTrama, VenceTimer, ErrorCS)
proceso emisor;
var    s: trama;    b: paquete;    suceso: SucesosPosibles;
        siguiente: (0,1);
inicio
    siguiente:=0;
    De_N3(b);

```

```

repetir
  s.info:=b;    s.sec:=siguiente;
  A_N1(s);
  InicioTimer;
  espera(suceso);
  Si suceso=LlegaTrama
    De_N3(b);
    aumentar(siguiente);
  finsi;
hasta siempre;
fin;    (* proceso emisor *)

```

```

proceso receptor;
var    r,s: trama;
        suceso: SucesosPosibles;
        esperado: (0,1);
inicio
  esperado=0;
  repetir
    esperar(suceso);
    Si suceso=LlegaTrama
      De_N1(r);
      Si r.sec=esperado
        A_N3(r.info);
        aumentar(esperado);
      finsi;
      A_N1(s);
    finsi;
  hasta siempre;
fin;    (* proceso receptor *)

```

Si el tiempo del temporizador es muy corto y vence antes de que le lleguen el reconocimiento se pierden tramas.

Protocolos de ventana deslizante

Consideraciones a tener en cuenta:

- La transmisión ya no es simplex sino que se transmite información en ambos sentidos (duplex o semi-duplex)
- Van a haber tramas de datos y reconocimiento mezcladas en el canal, para diferenciarlas se usará el campo clase.
- Se usará una técnica de reconocimiento llamada PIGGIBACKING, consiste en enviar el reconocimiento junto a la trama de datos.
Problema: si no hay tráfico de sentido inverso. Se deberá habilitar un temporizador para esperar un cierto tiempo si hay datos para enviar, en caso contrario se enviará una trama de reconocimiento.
Ventajas: al haber menos tramas se realizará un mejor uso del canal.
- Todas las tramas están identificadas por un número de secuencia entre 0 y 2^n-1

- Permiten el envío de varias tramas antes de que las estaciones se queden bloqueadas esperando el reconocimiento.
- Las estaciones que utilizan estos protocolos mantienen una ventana de emisión (lista con los números de tramas enviadas por esa estación y que están pendientes de reconocimiento) y una de recepción.

El hecho de enviar varias tramas antes de que se bloquee la estación implica el tener unos buffers con las tramas enviadas por si se deben volver a enviar, esto añade cierta complejidad a los protocolos.

La ventana de recepción contiene una lista con los números de secuencia de las tramas que puede aceptar la máquina receptora.

TEMA 5 EL NIVEL DE RED

5.1 Introducción

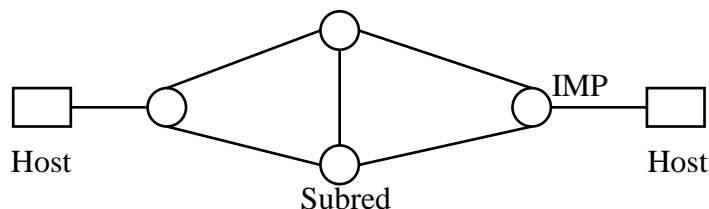
El nivel de red se ocupa del manejo de bloques de datos desde la estación origen a la estación destino. Las entidades de nivel 3 deben ser capaces de distinguir la topología de la red y encontrar el camino más adecuado para comunicar el origen con el destino.

Las condiciones de encaminamiento deben tomarse teniendo en cuenta el funcionamiento de la red. Puede darse el caso de que emisor y receptor estén en redes distintas.

Funciones del nivel de red:

- funciones de encaminamiento,
- comprobar que no se originen problemas de congestión,
- interconectar distintas redes.

La principal misión del nivel de red es proporcionar servicios al nivel de transporte.



IMP: procesador dedicado a las comunicaciones.

Como la subred es un conjunto de entidades, los servicios del nivel de red son los servicios que ofrece la subred.

En un caso ideal, lo que se desea es que los servicios del nivel de red cumplan las siguientes características:

- independientes de la estructura de la subred,
- el nivel de transporte no tiene que conocer el número, tipo o topología de las subredes que atraviesan sus datos,
- deben poner a disposición de sus usuarios un esquema de direccionamiento uniforme.

Estructura subred	Servicios	
Conmutación circuitos	Con conexión Sin conexión	
Conmutación paquetes	Sin conexión Con conexión	Datagrama Circuito Virtual

¿Cómo construir un circuito virtual sobre una red de conmutación de paquetes?

Cada datagrama se puede encaminar por separado pero todos deben llevar en su cabecera la dirección de destino.

Si se utiliza un circuito virtual cada paquete llevará una identificación del circuito virtual en lugar de la dirección de destino. En la fase de establecimiento del circuito se toman las decisiones de encaminamiento. Normalmente se empleará mejor el ancho de banda cuando se utilice un circuito virtual, además en este caso todos los paquetes llegan en el mismo orden en que fueron enviados.

Ventaja de los datagramas: mejor control del encaminamiento.

Cómo se establecen los circuitos virtuales:

Cada IMP mantiene una serie de tablas donde se almacena la información de los circuitos virtuales que atraviesan cada uno de estos IMP. Para esto tenemos dos opciones:

1. Utilizar un número diferente para cada circuito virtual, aunque no es la más correcta.
- 2.

5.2 Algoritmos de encaminamiento

El nivel de red está justificado cuando existe una subred. Las decisiones de encaminamiento se basan en una estimación de la distancia entre el host que toma la decisión y el host destino. Se toman en base a una métrica establecida. Métricas:

- número de saltos entre nodos
- capacidad de los canales
- distancia entre nodos
- retardo medio de transmisión y almacenamiento

Las decisiones de encaminamiento se toman en el momento del establecimiento del circuito virtual o cuando se recibe un paquete en el caso de datagramas.

Los algoritmos de encaminamiento se dividen en dos tipos:

1. **Algoritmos adaptativos**, permiten cambiar sus decisiones en función de variaciones en la topología o tráfico de la subred. En función de en qué lugar se recoja la información que va hacer variar las decisiones, se dividen en:

- *algoritmos centralizados*, usan información de toda la subred pero requieren de un controlador central que se encarga de tomar las decisiones y distribuirla a todos los IMP.
- *algoritmos aislados*, usan información local a ese IMP (longitud de las colas de salida, ...)
- *algoritmos distribuidos*, son una mezcla de ambos, basan sus decisiones en información de los IMP próximos.

2. Algoritmos no adaptativos (estáticos), son aquellos que se plantean a priori y se cargan en los IMPs, que siempre funcionan igual independientemente de que se produzcan cambios en la topología o en el tráfico que atraviesa la subred.

Encaminamiento por inundación

Cuando un IMP recibe un paquete lo envía por todas las líneas excepto por aquella que le ha llegado. Provoca la saturación de la subred sino se limita, ya que existen muchos duplicados.

Ventaja: seguro que llega a su destino y por el camino más corto.

Utilizado en interconexión de redes de área local. Se puede utilizar con algunas modificaciones que mejoran su rendimiento, paquetes con contador de saltos que se va decrementando en cada salto y llegan a eliminarse de la red cuando el contador llega a cero. Un buen número para el contador es el del diámetro (camino más largo que hay entre dos IMPs) de la subred

Otra mejora: añadir un número de secuencia a cada paquete que el IMP recibe del host para que solo transmita el paquete una vez. En este caso existe el problema de que los IMP deben saber los números de secuencia que han utilizado.

Algoritmo no adaptativo, ya que las decisiones de encaminamiento están decididas a priori.

Encaminamiento por el camino más corto

El IMP cuando le llegue un paquete lo enviará por el camino más corto que lo una con el destino, para esto hace uso de una de las métricas vistas anteriormente.

El algoritmo será estático si se coloca las distancias a priori en cada IMP, pero si se produce un refresco de estas distancias, el algoritmo será adaptativo.

Cada IMP tiene una tabla de encaminamiento, en la que se indica por que línea saldrá cada paquete según su destino.

A	L1
B	L2
...	...

Pueden existir otras tablas de encaminamiento más flexibles:

Destino	Línea P	Línea P	Línea P
A	L1 0.4	L3 0.4	L4 0.2

En caso de que caiga alguna línea, existirá la probabilidad de encaminar el paquete.

Encaminamiento centralizado (Enc. Delta)

Existe un controlador central de encaminamiento, un IMP recibe información de la red y construye las tablas de encaminamiento y las manda a los IMP.

Problema: si cae el organismo central deja de funcionar.

Los IMP deben de enviar información al controlador central por lo que parte del ancho de la subred se usa en su gestión. Si queremos que el sistema sea flexible y se cambie con frecuencia se tendrá mucho tráfico de información con datos para la gestión de la subred.

En el encaminamiento delta, cada IMP mide el coste de cada una de las líneas de salida enviando paquetes de prueba, con esta información se hace un paquete y se manda al controlador central, el cual con esta información que recibe calcula los k mejores caminos que unen cada par de IMPs que forman parte de la subred.

C_{ij} coste del mejor camino entre i y j
 C_{ij}^k coste del k -ésimo mejor camino entre i y j

Con esos caminos y un parámetro δ determina que todos los caminos que cumplan $|C_{ij}^n - C_{ij}^1| \leq \delta$ se consideran caminos equivalentes entre i y j .

Con esto se transmiten las tablas y cada IMP toma las decisiones entre los caminos equivalentes.

El ajuste del parámetro δ marcará:

- si δ muy pequeña \Rightarrow pocos caminos equivalentes y el margen de maniobra de cada IMP será pequeño.
- si δ es mucho mayor que cero \Rightarrow habrá muchos caminos equivalentes entre los que decidir el IMP local.

El algoritmo es centralizado pero según el parámetro δ puede ser más o menos distribuido.

Encaminamiento aislado

Las decisiones de encaminamiento las toma cada IMP de forma local. En función del destino escogerá la línea adecuada basándose en información local. El algoritmo es adaptativo (o al menos puede serlo). Puede verificar el estado de las colas de salida o comprobar el estado de los enlaces para encaminar los paquetes.

Tiene dos variantes:

- **Algoritmo de la patata caliente:** los paquetes se encaminan por la línea que tiene la cola menor. No se tiene en cuenta el destino, por lo que es muy poco eficiente. Puede ser útil en combinación con otros algoritmos, como por ejemplo el algoritmo del camino más corto.
- **Algoritmo de aprendizaje retrospectivo:** cada paquete lleva dirección origen y destino y al llegar cada paquete puede ir construyendo sus tablas de alcanzabilidad (según líneas). Si llega un paquete de Y , por la línea Y , sabremos que Y será alcanzable por Y ¿Será adaptativo? En cierto modo si, siempre y cuando le llegue un paquete por otra línea. Las tablas deben actualizarse periódicamente. Es ampliamente utilizado en LAN. Si llega un paquete que no sabe dónde enviar, utiliza inundación. Es una combinación de inundación y aprendizaje retrospectivo, lo que se utiliza en puentes transparentes de LAN.

Mejora: aprender de los orígenes y saber además lo lejos que está (con un contador de saltos). Deberá tener una tabla con todos los destinos y todas las líneas para tener todas las posibles configuraciones. Puede que no lleguen paquetes por todas las líneas, con lo que la tabla estará incompleta, pero las decisiones se tomarán en base a los datos disponibles.

Encaminamiento distribuido

La información que utiliza el IMP está basada en información local más información recibida de otros IMP cercanos a él. Todos los IMP saben cuales son sus adyacentes, será posible mediante intercambios de información

Problema: hay una parte del ancho de banda que está consumido por el tráfico de tablas en la subred.

Encaminamiento jerárquico

En redes de gran tamaño con muchos IMP se necesitan grandes recursos para mantener las tablas de encaminamiento y el tipo de proceso de los IMP también será mayor. Una solución es dividir la subred en áreas, donde cada IMP sólo tiene información de su área y cómo acceder a las restantes áreas.

Así, la tabla de encaminamiento no necesita una entrada para cada destino, sino que tiene una entrada por IMP de su región y una para cada región.

Utilizado en internet. El coste es que para una determinada región no se elija el mejor camino para algunos IMP concretos. Las subredes de este estilo suele haber más de dos únicos niveles.

5.3 Control de la congestión

Degradación que se produce cuando tiene demasiados paquetes circulando por la subred.

Tráfico ofrecido: cantidad de información que los hosts vierten en la subred para su encaminamiento. La subred tiene una capacidad máxima limitada, ya que sus componentes están limitados.

El número de paquetes que la red ha procesado es el **tráfico cursado**. Cuando el tráfico ofrecido llega a la capacidad de la subred se produce la congestión y el funcionamiento de la red deteriora. Además la congestión se realimenta y empeora en funcionamiento.

La congestión puede producirse por:

- congestión de IMP, se llena la cola de un IMP, el emisor intenta reenviar, no vacía los buffers, ...
- insuficiente capacidad de proceso en los IMP
- velocidad insuficiente de las líneas de salida. Si las líneas de salida son muy lentas se colapsará el IMP porque recibirá muchos datos y no los podrá enviar.

Una causa más general es tomar malas decisiones de encaminamiento. Pueden sobrecargar un IMP determinado. La diferencia con el control de flujo del nivel 2 es que ahora hablamos de la subred como un conjunto.

Mecanismos para evitar la congestión:

- Reservas de buffers (en subredes de circuito virtual). Al mismo tiempo que se crea el circuito se reserva espacio para los paquetes que van a circular por ese circuito virtual. Si un determinado paquete ya no cabe, puede intentar crear otro circuito.
- Rechazo de paquetes (en redes con servicio de datagrama), cuando un IMP no puede procesar un determinado paquete simplemente lo rechaza y se encamina por otro lado.
- Limitar el número de paquetes que pueden circular o “control isarrítmico de la congestión”. Se ponen a circular unos paquetes de permiso. Cuando un host quiere transmitir retira uno de estos paquetes, envía, el destino recoge los datos los procesa y regenera el paquete de permiso. Esto garantiza que el número de paquetes es fijo pero igual se puede congestionar

un IMP. Además, ¿cómo se hacen circular los paquetes para que toda estación pueda transmitir? y además, si se pierde un paquete estamos limitando el tráfico por debajo del máximo \Rightarrow mecanismo de purga y reinicialización de la red.

- Paquetes de restricción, cada IMP monitoriza sus líneas de salida y hace una estimación de su uso, si se sobrepasa un umbral, avisa a las estaciones que le obligan a utilizar esa línea de salida mediante un paquete de restricción. El host origen disminuirá en un % el tráfico hacia el host destino.

La utilización de las líneas de salida se miden con la expresión:

$$u_t = a \cdot u_{t-1} + (1-a) f$$

$f = 0$ (libre) o 1 (ocupado)
 $u = 0 \dots 1$
 $a = \text{constante}$

5.4 Protocolo IP

Internet Protocol

TCP/IP son un conjunto de protocolos

Telnet	FTP	Http
TCP / UDP		
IP	ICMP	
	ARP	
	RARP	

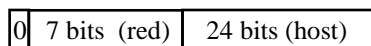
Todos estos protocolos se originaron en los años 80

IP es un protocolo sin conexión y no fiable. A la unidad de datos del nivel de red, el protocolo IP la denomina datagramas

Direccionamiento IP

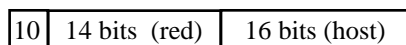
Una dirección IP está compuesta por dos partes: un identificador de red y un identificador de host. Todas las direcciones IP se componen de cuatro octetos, y en función del espacio destinado a cada parte se definen varias clases de direcciones:

Direcciones de clase A: formadas por un octeto para el identificador de red y tres para el identificador del host. Se caracterizan porque el primer bit es un cero.



Se pueden crear 125 redes de clase A, ya que la dirección todo ceros y todo unos no se puede utilizar.

Direcciones de clase B: formadas por dos octetos para el identificador de red y dos para el identificador del host. Se caracterizan porque comienzan por 10.



Tendremos $2^{14} - 2$ redes, cada una de ellas de 65.534 máquinas.

Direcciones de clase C: formadas por tres octetos para el identificador de red y un único octeto para el identificador del host.

110	21 bits (red)	8 bits (host)
-----	---------------	---------------

Tendremos 2.097.152 redes de 254 máquinas cada una.

Al igual que en los casos anteriores no son válidas las direcciones de host formadas todas por ceros o por unos.

NIC (Network Information Center) organismo encargado de gestionar las direcciones de Internet.

La dirección de red se indica poniendo los octetos del host a cero. Una dirección con todos los bits del host a uno hace referencia a todas las máquinas de la red.

Direcciones de clase D: direcciones multicast, hacen referencia a un grupo de estaciones destinatarias.

1110	
------	--

Puede darse el caso de que no se ajuste la dirección asignada a nuestras necesidades, para esto tenemos la máscara de subred que indica el número de bits de una dirección IP que se destinan al identificador de red.

Máscara de subred para direcciones de la clase A: 255.0.0.0
 B: 255.255.0.0
 C: 255.255.255.0

Es posible utilizar parte de los bits que en principio identificarían al host para identificar la red. En lugar de usar la máscara de bits por defecto se amplía el número de bits.

Ejemplo: Clase B

150	128	0	0	dirección IP
111111	111111	0 . . . 0	0 . . . 0	máscara por defecto
111111	111111	10 . . . 0	0 . . . 0	máscara extendida

Esto indicará que habrá dos redes:

150.128.00 . . . 0
 150.128.10 . . . 0

No se puede usar un solo bit para extender la máscara, en este caso se debería expandir la máscara en dos bits.

~~150.128.00x . . . x~~ no se puede usar
 150.128.01x . . . x
 150.128.10x . . . x
~~150.128.11x . . . x~~ no se puede usar

150	128	00		
		01		$2^{14} - 2$
		10		$2^{14} - 2$

Siempre que se usa una máscara extendida se perderá espacio de direccionamiento.

150.128 en dos subredes $2 \times (2^{14} - 2)$
en seis subredes $6 \times (2^{13} - 2)$

Cuando más extendamos la máscara, menos espacio de direccionamiento perderemos.

¿Cómo sabe una estación si otra está en la misma red que ella?

Mirando la parte de la dirección que identifica la red.

150.128.13.21 máscara 255.255.224.0
150.128.200.215

Sabemos si están en la misma red haciendo un AND entre las direcciones de las estaciones y la máscara y comprobando que obtenemos el mismo resultado, es decir, la dirección de la red.

Razones para dividir una red en varias subredes:

- eficiencia
- seguridad
- mejorar la gestión

En la máscara de la subred se marca con unos los bits del identificador de red y con ceros los bits del identificador del host.

Cuando utilicemos direcciones IP no podremos usar direcciones con todo ceros o todo unos en el identificador de red, el del host o en la máscara de la subred.

Cuando se intercambia información entre dos estaciones dentro de la misma red se utilizan encaminamiento directo, en cambio si las estaciones no se encuentran en la misma red se usa encaminamiento indirecto ya que se necesita la participación de un tercer elemento denominado gateway o router (encaminador).

Ejemplo:

Suponemos que tenemos una dirección de clase B 129.1.0.0 y queremos dividir el espacio de direccionamiento en 250 redes distintas.

dir. IP	<table border="1"><tr><td>1000001</td><td>00000001</td><td>00000000</td><td>00000000</td></tr></table>	1000001	00000001	00000000	00000000	129.1.0.0
1000001	00000001	00000000	00000000			
máscara por defecto	1 . . . 1 1 . . . 1 0 . . . 0 0 . . . 0					
	1 . . . 1 1 . . . 1 1 . . . 1 0 . . . 0	255.255.255.0				

- Subred 1: 129.1.1.0
Subred 2: 129.1.2.0
.....
Subred 254: 129.1.254.0

Ahora queremos dividir el espacio de direccionamiento en 127 redes distintas.

dir. IP

1000001	00000001	00000000	00000000
---------	----------	----------	----------

 129.1.0.0

máscara por defecto 1 . . . 1 1 . . . 1 11111110. 0 . . . 0

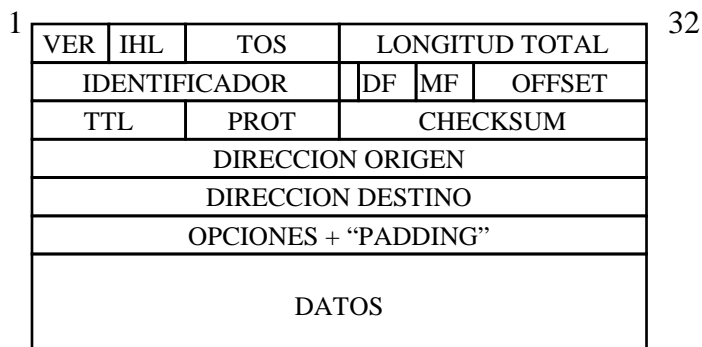
Subred 1: 129.1.2.0 desde 129.1.2.1 a 129.1.3.254

Subred 2 129.1.4.0 desde 129.1.4.1 a 129.1.5.254

.....

Subred 126: 129.1.252.0 desde 129.1.252.1 a 129.1.253.254

Datagrama IP



VER: (4 bits) versión del protocolo IP que ha originado el datagrama.

IHL: longitud del encabezamiento del datagrama medido en palabras de 32 bits. Valor entre 5 y 15 (4 bits)

TOS: Type of Service (8 bits)

			D	T	R		
--	--	--	---	---	---	--	--

Los tres primeros bits indican la prioridad 0= menor y 7 = mayor

D = 1 solicitud de bajo retardo

D = 0 solicitud de alta capacidad

R = 1 solicitud de alta fiabilidad

LONG. TOTAL: indica la longitud total del datagrama IP, en octetos.

Los datagramas IP no pueden tener menos de 576 octetos. Cuando el datagrama no quepa en alguno de los protocolos usados en alguna red, habrá que fragmentarlo.

Si se fragmenta un datagrama, todos los fragmentos llevarán el mismo identificador.

DF = 1 el datagrama no se puede fragmentar. Normalmente estará a cero.

MF (More Fragments): indica si el fragmento es el último del datagrama original, con un cero.

OFFSET: posición relativa del fragmento dentro del datagrama original, es un valor que se mide en unidades de 8 octetos (13 bits). Si el datagrama no está fragmentado es igual a cero.

TTL (Time to live), sirve para que lo marcan las estaciones que generan el datagrama con un valor y en cada salto se decremента en una unidad. Cuando llega a cero, el datagrama ya no se transmite más (8 bits).

PROT: indica el protocolo del nivel superior al que debe ser entregado el datagrama (8 bits) para TCP = 6

CHECKSUM: del encabezamiento (16 bits).

OPCIONES: campo de longitud variable, no obligatorio en los datagramas pero lo que si es obligatorio es la implementación del tratamiento de esas opciones en las entidades del protocolo.

Todas las opciones que pueden aparecer empiezan con un código de opción:

COPIA	CLASE	NUMERO OPCION
1 bit	2 bits	5 bits

COPIA = 0 \Rightarrow la opción no debe ser copiada en los fragmentos que se originen.

COPIA = 1 \Rightarrow se debe copiar la opción en los fragmentos.

CLASE = 00 \Rightarrow datagrama control de red

10 \Rightarrow medida y control de errores

Los otros dos están reservados

Opciones disponibles:

CLASE	NUM.	LONG.	OPCION	DESCRIPCION
0	0	1 byte	Fin lista opciones	Aparece siempre al final de las demás opciones
0	1	1 byte	No operación	Para ajustar las opciones a palabras de 32 bits
0	2	11 bytes	Seguridad	Codifica el nivel de seguridad y restricciones de acceso aplicables al datagrama
0	7	Var.	Grabación de ruta	Permite que la identidad IP que genera el datagrama cree una tabla vacía en la cual se graban las direcciones IP por las que pasa el datagrama
0	9	Var.	Encaminamiento desde origen	Permite a la estación origen establecer el camino que debe seguir el datagrama hasta llegar al destino
2	4	Var.	Time-stamping	Igual que la grabación de ruta, y además graba el tiempo en el que pasa.

Estructura de la opción “Grabación de ruta”:

Código	Long.	Puntero			
1 byte	1	1	4	4	4

El puntero siempre señalará la primera entrada de la tabla vacía
Long. Indica la longitud total de la opción.

Estructura de la opción “Time-Stamping”:

Código	Long.	Puntero	Desb	Flags
Dirección IP 1				
Tiempo 1				
Dirección IP 2				

Tiempo 2

Tiempo = día y milisegundos transcurridos desde la medianoche según el horario del meridiano de Greenwich.

Desb: indica las direcciones que ha atravesado el datagrama y no le han cabido en la tabla.

Flags: indica como deben los IMPs que atraviesa el datagrama grabar los datos.

- 0 sin dirección IP
- 1 dirección IP y momento del tiempo
- 2 direcciones IP colocadas por el remitente

Protocolo ICMP (Internet Control Message Protocol) es el que detecta los errores y los reporta al nodo que ha originado el datagrama. Para su transmisión los mensajes de este protocolo se encapsulan en datagramas IP.

El mensaje ICMP lleva información sobre la causa del error y los 64 primeros octetos del campo de datos del datagrama que ha causado el error.

Causas de error que producen mensajes ICMP:

- Tiempo de vida igual a cero, TTL = 0
- Parámetro desconocido en el encabezamiento
- Destino inalcanzable
- Congestión del nodo (“source quench”)

Otro problema con el que nos encontramos es la transmisión de datagramas IP sobre redes de área local.

El protocolo ARP (Address Resolution Protocol), cuando no sabe que dirección física corresponde a una dirección IP, envía una trama MAC a las demás estaciones que forman la red, indicando la dirección IP que busca. La estación que tiene esa dirección IP contesta indicando su dirección física.

La unidad de datos que intercambia el protocolo ARP indica:

Tipo Hardware		Tipo Protocolo
Long Dir Física	Long Dir Protocolo	Operación
Dirección Física Remitente		
		Dirección IP
Remitente		
Dirección Física Destino		
Dirección IP Destino		

El protocolo ARP intercambia direcciones MAC y direcciones IP.

RARP (Reverse Address Resolution Protocol)

Se usa en estaciones sin disco en las que no se les puede grabar su dirección IP, las cuales obtienen su dirección IP difundiendo su dirección física. Una estación mantendrá una tabla de equivalencia de direcciones y responderá con la dirección IP asociada.

DHCP (Dinamic Host Configuration Protocol)

Existe un servicio DHCP que manda las direcciones IP a las estaciones que quiere conocer su dirección.

5.5 Interconexión de redes

Cualquier dispositivo que se dedica a la interconexión de redes lo denominaremos relé.



Relé: dispositivo físico y lógico que sirve para llevar a cabo la unión de dos redes a cualquier nivel.

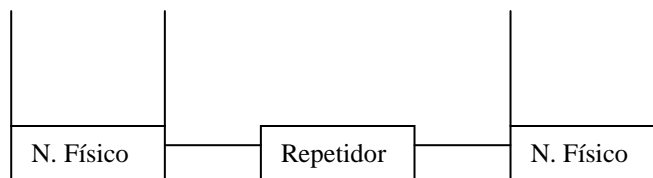
Clasificación de los relés:

<u>Nivel OSI</u>	<u>Relé</u>
Físico	Repetidor
Enlace	Puente (Bridge)
Red	Encaminador (Router)
Transporte o superiores	Pasarela (Gateway)

Gateway denominado también conversor de protocolo.

1º) Repetidor

Dispositivo más elemental para la conexión de dos redes. Actúa a nivel 1 y sirve para regenerar la señal que transmite los datos. Son dispositivos hardware sin posibilidad de configuración.

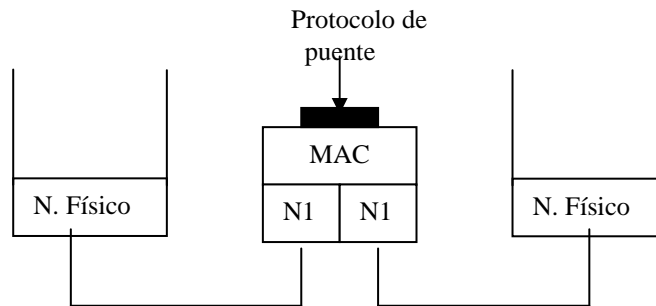


Los dos medios físicos que conecta deben ser iguales

2º) Puentes

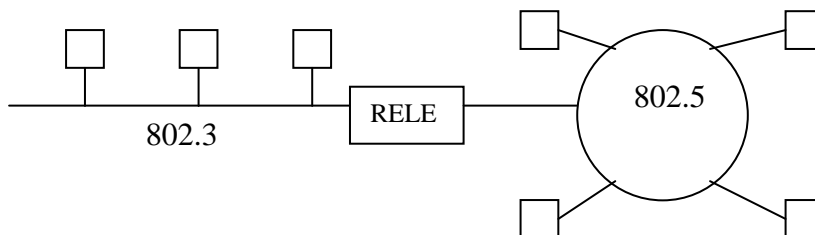
Son un relé que opera a nivel de enlace.

- Un puente podrá conectar dos redes ethernet.



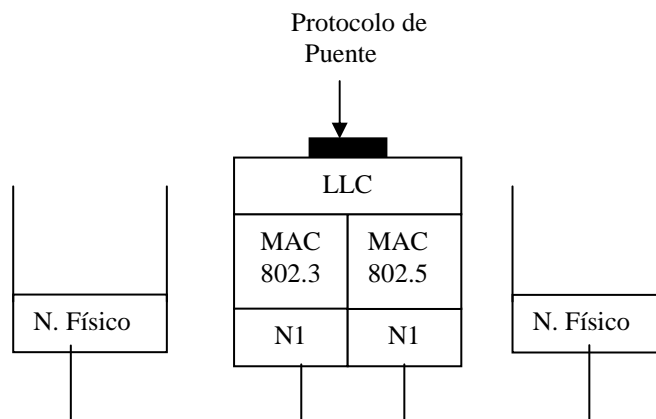
En ambos casos las dos redes tienen el mismo subnivel de acceso al medio (MAC). El puente no modificará ni el contenido de las tramas ni su formato, simplemente decidirá si una trama que circula por un medio físico va a pasar al otro segmento o no. Solamente se añadirá una pequeña parte denominada protocolo de puente, que es quien tomará las decisiones.

- ¿Podrá conectar una red de tipo 802.3 y otra de tipo 802.5?



Cada red tiene diferente topología, diferente formato y longitud de trama, diferentes velocidades de transmisión, la 802.5 establece un sistema de prioridades que no establece la 802.3. En la 802.5 las tramas indicaban si había sido reconocidas y copiadas, algo que en este caso deberá realizar el relé.

El relé deberá tener dos subniveles de acceso al medio distintos.



El nivel físico capturaré la trama y la pasará al MAC que la reconoce y extrae el campo de datos y lo pasa al control de enlace lógico que encapsulará toda la información en una trama de la red a la que se va a pasar esa información.

Una trama del segmento de red 802.5 puede dar lugar a varias tramas del segmento 802.3

Los puentes más comunes son los que unen dos redes iguales.

¿Por qué puede ser interesante unir distintos segmentos de red?

- **Fiabilidad:** si tenemos muchos equipos conectados a una red, un corte en el cable deja inservible toda la red, en cambio si se segmenta la red solo produciría problemas en su segmento.
- **Prestaciones:** si se realiza una buena división de la red de manera que se consiga minimizar el tráfico intersegmentos y maximizar el tráfico intrasegmentos.
- **Seguridad:** a veces es conveniente que el tráfico de una red no sea accesible desde otro segmento de la red.
- **Ubicación geográfica:** si cada segmento de red está separado de los demás, será necesario recurrir a dispositivos que proporcionen esa conexión remota.

Arquitectura de un puente

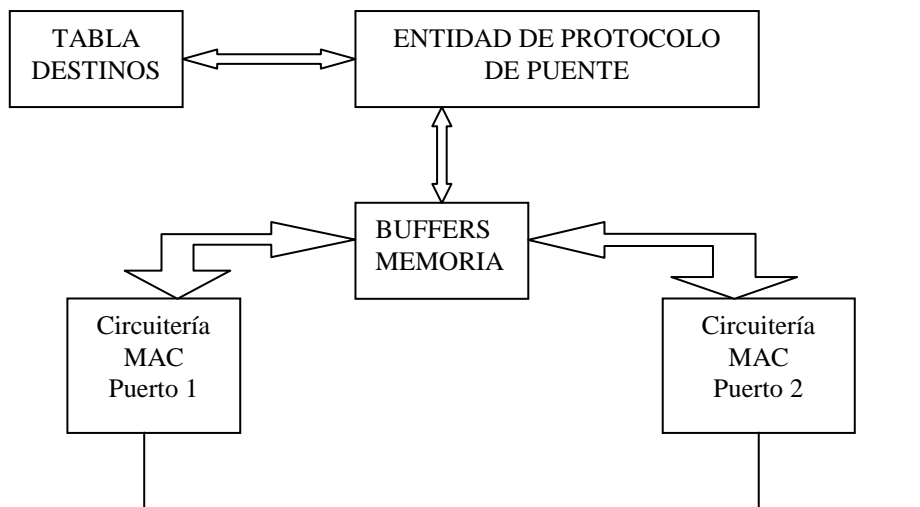


Tabla de destinos ayudará a decidir a la entidad de protocolo de puente por qué puerto saldrá la trama.

TABLA DESTINOS

Puerto	Dirección	Tiempo
1	08-AA-CC ...	
2	08-AC ...	

Puentes transparentes

Se basan en el principio de que para hacerlo funcionar solo hace falta conectarlo a los dos segmentos que se quiere conectar, no hace falta configurarlo.

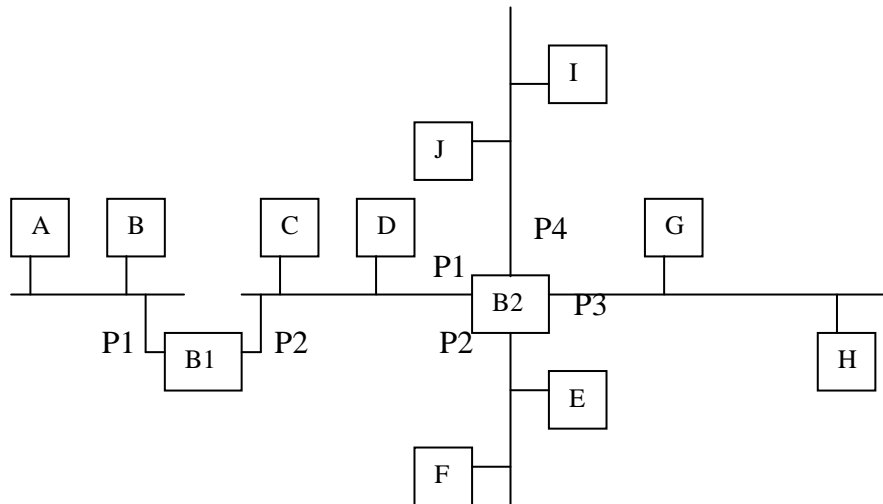
Lo único que requiere es que las redes respeten el estándar de direccionamiento 802

En su operación se distinguen tres fases:

1. **Retransmisión,** si el puente no sabe dónde está la estación destino inunda todos los segmentos con la trama excepto por el que le ha llegado. Si el puente ya sabe donde está la estación destino simplemente la retransmite hacia el segmento de red donde se encuentra la estación destino.

2. **Aprendizaje retrospectivo**, el puente extrae información de las tramas que le van llegando.
3. **Control de bucles**

Ejemplo:

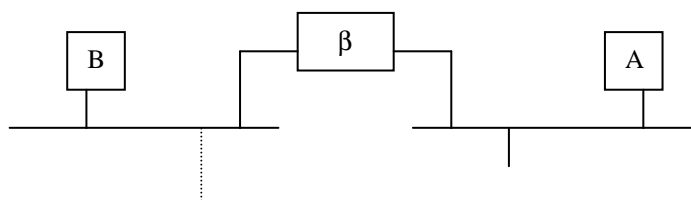


- Suponemos que se transmite una trama desde la estación A a la E.
 B1 leerá la dirección destino de la trama y la retransmitirá por P2 y provocará que la tabla de destinos se actualice colocando la dirección destino A por el puente P1
 B2 capturarà la trama por P1, como en la tabla de destinos no hay nada, la retransmitirá por todos los puertos menos por el que le ha llegado y actualizarà su tabla de destinos con la dirección de origen de esa trama.
- Transmite una trama de E hasta A
 Capturarà B2 la trama, como la dirección de destino la tiene en su tabla la transmitirá por su puerto asociado en la tabla P1 y pondrá en la tabla la dirección origen.

Si se cambia una estación de red, tendremos una entrada errónea en la tabla de la red hasta que esa estación mande una trama o venza el temporizador asociado a dicha entrada de la tabla, en cuyo caso se borra la entrada.

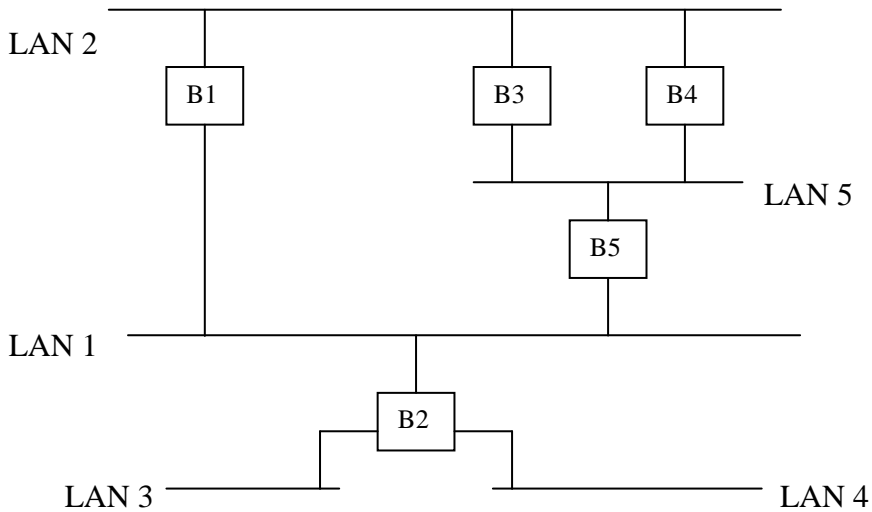
Control de bucles

Se ponen dos puentes por razones de seguridad y fiabilidad. Para evitar los bucles debemos conseguir que solo funcione un puente y que el otro solo entre en funcionamiento si falla el otro.





Para que esto funcione se usa el algoritmo “spanning-tree” de forma que se define un camino único para dos segmentos de red y así se evitan los bucles.

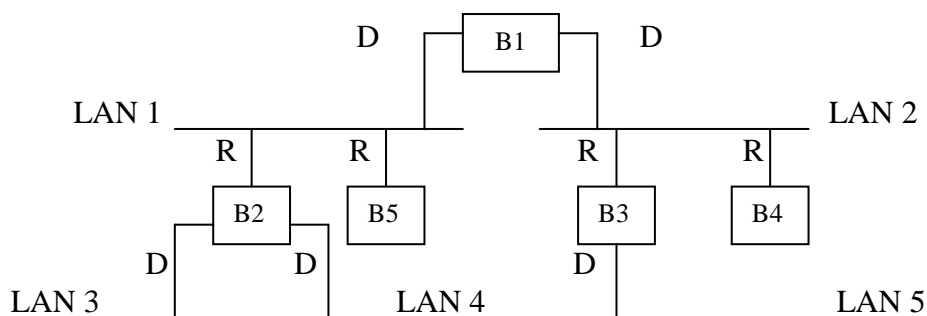


¿Cómo aplicamos el algoritmo en este caso?

Cuando aplicamos el algoritmo los puentes transparentes dejan de serlo, ya que los puentes necesitan un identificador único dentro de la red. Además será necesario definir unas direcciones multicast que permitan intercambiar información entre los puentes. También será necesario identificar dentro de cada puente sus puertos con un identificador único.

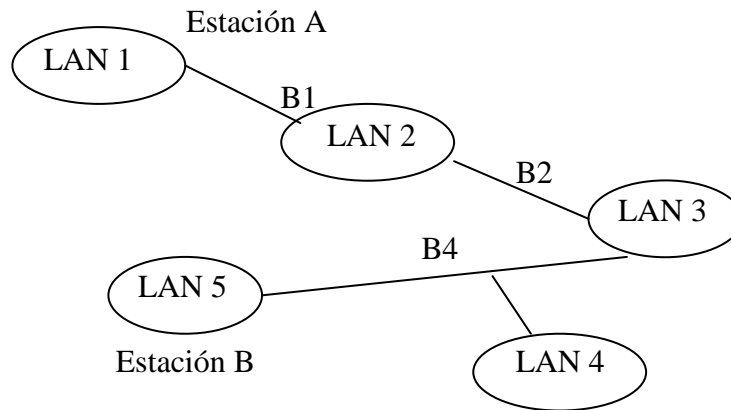
Pasos a seguir para construir el árbol de expansión:

- Definir el puente raíz, el que tiene el identificador más bajo (B1)
- Costo de comunicación entre cada uno de los puentes y el puente raíz, se puede calcular de diversas maneras o puede ser configurado por el administrador.
- Cada puente debe ser capaz de determinar cual es su puerto raíz, el que le permite enlazar con el puente raíz por el camino de menor costo.
- Todos los puentes tienen unos puertos designados, para cada segmento de LAN hay un puerto designado, que es a través del cual se envían y reciben tramas a ese segmento de red.



Si cae B3 se podrá acceder a la LAN 5 a través de B4 o B5

Los puentes transparentes se utilizan en redes del tipo 802.3, mientras que en redes 802.5 se usan puentes con encaminamiento desde el origen (source route), estos asumen que la ruta completa fuente-destino está presente en todas las tramas interredes, luego cada estación debe conocer la ruta completa has todos los posibles destinos.



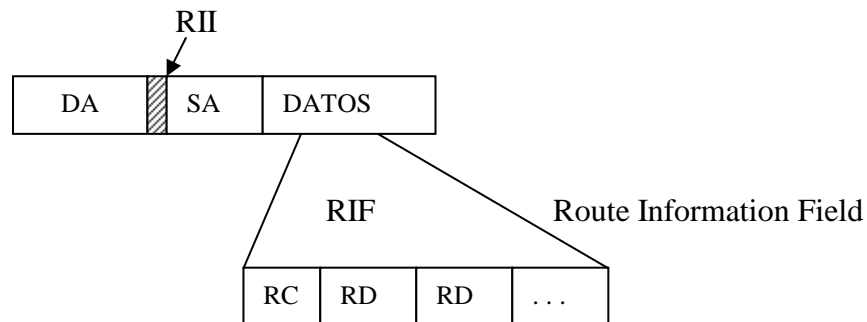
La ruta entre las estaciones A y B constará de:

B1-LAN2 B2-LAN3 B4-LAN5

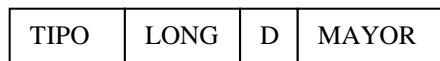
Cada puente se identifica con 4 bits y una red con 12 bits. Luego una ruta estará formada por varios pares de octetos (puente/red)

Esta información va en el campo de datos de la trama, lo cual se indica a través de un bit RII (routing information indicator), que es el bit más significativo del campo dirección de origen.

Direcciones MAC, primer bit indica si la dirección es única (0), o de un conjunto de estaciones (1).



RC (Route Control)



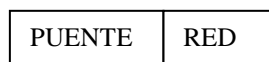
TIPO = estaciones a las que va la trama

LONG = longitud del campo RIF en octetos

D = indica si la trama va o vuelve

MAYOR = indica el mayor tamaño de trama que puede atravesar el anillo

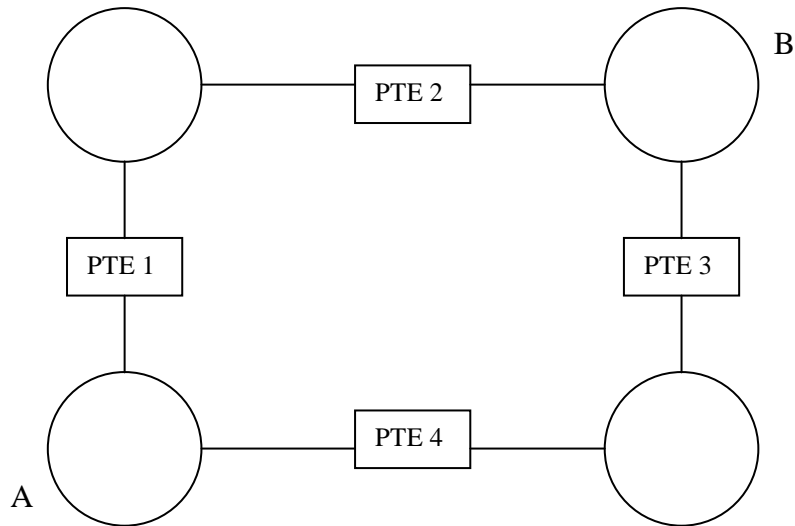
RD (Route Descriptor)



4

12

Funcionamiento de estos puentes:



La estación A quiere enviar una trama a la estación B:

1º) Averiguar si la estación B está en el mismo anillo, enviando una trama de exploración dentro del propio anillo.

2º) Enviar la trama fuera del anillo

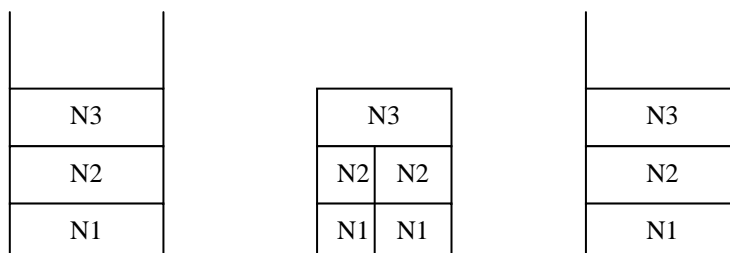
- Si A sabe la ruta completa hasta B, marcará el bit RII a 1 y grabará toda la ruta en el campo de datos.
- Si A no sabe la ruta hasta B, envía tramas de exploración fuera del anillo. Hay dos tipos de tramas de exploración:
 - SRB (Single Route Broadcast)
 - ARB (All Route Broadcast)

En primer lugar se envían tramas SRB y se construye un árbol de expansión. Cuando una de estas tramas llega a B, ésta contesta con tramas ARB con dos condiciones:

- Contador de saltos
- Que una trama no pase dos veces por el mismo anillo

A la estación A le llegarán varias tramas con la ruta marcada y elegirá una (la primera en llegar, la que le permita una mayor tamaño de trama, etc.)

Routers

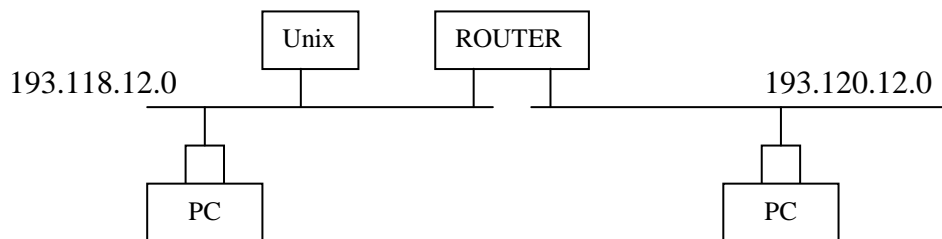




El hecho de operar a nivel de red da la posibilidad de intercambiar tramas entre redes muy distintas. Su funcionamiento es un poco más lento que los puentes ya que necesitan más tiempo de proceso.

Los routers se usan para constituir redes de área extensa. Muchas veces aparecen como dos equipos unidos mediante una línea de comunicación, lo que se denomina semipuentes o semirouters.

Los Brouters utilizan el nivel 3 para determinados protocolos y otros se usan a nivel 2, es decir, algunos protocolos se puentean y otros se enrutan.



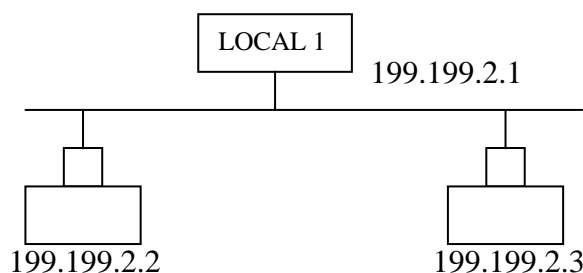
El router tiene una tabla de direcciones de red que le indica si debe pasar una trama a la otra red o no.

Los routers son los encargados de la fragmentación ya que conectan las dos redes y saben el tamaño máximo de los paquetes que pueden circular por ellas.

- **Fragmentación transparente:** el router fragmenta los paquetes que le llegan si es necesario.
Ventaja: las estaciones no se preocupan del problema de la fragmentación
Problemas: se pierde la posibilidad de usar la red de forma más eficiente, no se pueden usar rutas distintas para los diversos fragmentos de un paquete.
- **Fragmentación no transparente:** cuando el router de entrada a una red recibe un paquete que no cabe en esa red, lo fragmenta pero nadie lo reconstruye sino que es la estación final la encargada de sacar todos los datos de los fragmentos.
Ventaja: los paquetes se pueden encaminar de una manera óptima.
Problema: todas las estaciones deben ser capaces de reensamblar los paquetes, además la carga de la red aumenta. Otro problema es el de la identificación de los fragmentos.

IGRP (Internet Gateway Routing Protocol), sirve para que los routers intercambien sus tablas de encaminamiento.

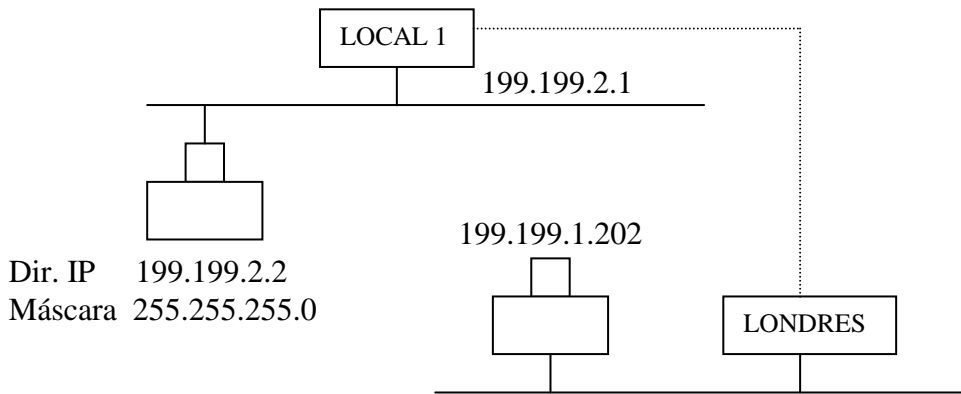
DNS, sistema que produce las traducciones entre los nombres y las direcciones IP.



Para que puedan comunicarse estas dos estaciones, la estación de origen debe conocer la dirección MAC de destino, para ello vierte una trama ARP en el medio con la dirección IP de la estación destino, la cual contestará con su dirección MAC.

¿Qué pasa si la dirección destino es otra red? 199.199.3.0

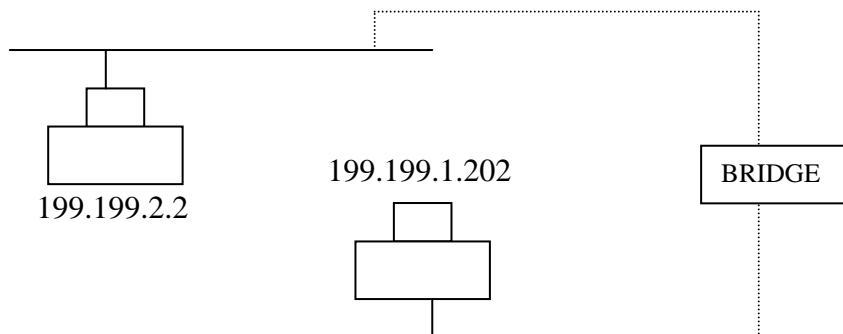
Se seguirá el mismo mecanismo anterior



¿Cómo se comunican estas dos máquinas?

La estación origen comprueba si la estación destino está en su misma red, como no es así, entonces es necesario recurrir al router, para ello se debe averiguar la dirección MAC del router a partir de la dirección IP.

Una vez le llega la trama al router, éste consultará sus tablas y mandará la trama por un de sus líneas de salida.



La estación origen construirá una trama ARP para conocer la dirección MAC de destino, el puente difundirá la trama por todas sus salidas y la estación destino contestará.

Si usamos un router y no queremos que una trama no salga de un segmento se puede conseguir, en cambio usando puentes transparentes una trama se puede transmitir por varios segmentos.

Antes de aplicar el protocolo ARP se debe asegurar que la estación destino está en la misma red, para ello se aplica el AND bit a bit de la dirección destino con la máscara.

199.199.1.1		199.199.1.252	
<u>255.255.255.0</u>	AND	<u>255.255.255.0</u>	AND
199.199.1.0		199.199.1.0	

TEMA 6 EL NIVEL DE TRANSPORTE

TCP es un protocolo orientado a la conexión, es fiable. Se encarga del control de flujo y errores a través de una subred.

La unidad de datos de este protocolo se llama segmento. Un segmento lleva un checksum del encabezamiento y de los datos, esto es lo que hace que sea fiable.

El nivel de transporte y el de red están íntimamente ligados.

La fiabilidad dependerá del ámbito de la red.

SEGMENTO TCP

PORT ORIGEN		PORT DESTINO	
NÚMERO SECUENCIA			
NÚMERO RECONOCIMIENTO			
OFF.	RES	COD.	VENTANA
CHECKSUM		PTR. URGENTE	
OPCIONES		PADDING	
DATOS			

PORT: direcciones del nivel de transporte

Nº SECUENCIA: asigna un número de secuencia a cada octeto individual. Identifica todos los octetos de una conexión.

Nº RECONOCIMIENTO: contiene el valor del número de secuencia del siguiente octeto que espera recibir la máquina que ha originado el segmento.

OFFSET: (4 bits) indica la longitud en palabras de 32 bits del encabezamiento del segmento.

RES: (6 bits) reservados, no se usan.

CODIGO:

- bit 11 URG indica cuando está a 1 que el campo PTR. URGENTE es significativo, que existe tráfico fuera de banda. El contenido de PTR. URGENTE indica donde empiezan los datos de la aplicación, datos normales.
- bit 12 ACK reconocimiento significativo, cuando está a 1 indica que el campo número de reconocimiento es significativo.
- bit 13 PSH push, a 1 indica a la estación receptora que debe pasar los datos inmediatamente al nivel superior.
- bit 14 RST reset conexión
- bit 15 SYN sincronización. La apertura de una conexión se realiza con el envío de un segmento con este flag a 1 y el número de secuencia, destino acepta y devuelve SYN = 1 y ACK = 1
Este se llama protocolo de establecimiento de la conexión a 3 bandas.
- bit 16 END indica el fin de la transferencia de datos en ese sentido.

VENTANA: marca el tamaño de la ventana de emisión, marcado por la entidad receptora.

CHECKSUM: comprobación del encabezamiento y de los datos.

El reconocimiento que usa TCP se denomina reconocimiento acumulativo.