

Capítulo 1:

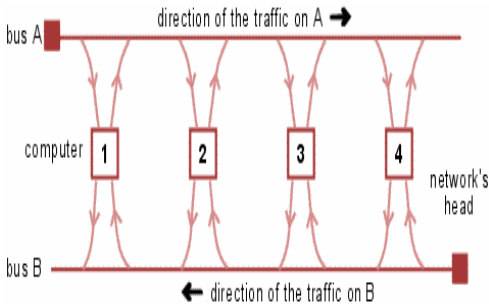
Evolución Histórica:

- **Modelo OSI** (Open Systems Interconnection): La ISO (International Standards Organization) crea el subcomité ISO/TC 97/SC16. El resultado del cual fue el desarrollo de una serie de estándares denominado Modelo Básico de Referencia para la Interconexión de Sistemas Abiertos.
- **ATM** (Asynchronous Transfer Mode): Red de 1990 que transfiere Mbps.
- **Modelo TCP / IP** (Transmission Control Protocol / Internet Protocol): Describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red y provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

Tipos de redes:

- **Redes de Difusión:** Existe un único canal de comunicación compartido por todas las máquinas de la red. Los mensajes transmitidos por una máquina de la red al medio de comunicación son recibidos por todas las demás. Se realiza indicando un código especial en el campo de dirección del mensaje para que todas las máquinas puedan procesarlo.
- **Red de Multidifusión:** La señal emitida (mensaje) por un transmisor es recibida por cualquier subconjunto de máquinas conectadas a la red. Se reserva un bit del campo dirección en el mensaje para indicar multidifusión siendo los n-1 bits restantes del campo de dirección empleados para direccionar grupos de máquinas en la red.
- **Red Punto a Punto:** Se establecen múltiples conexiones entre pares individuales de máquinas. Para realizar la transmisión es posible que el mensaje deba visitar máquinas intermedias. Como existen rutas alternativas para la comunicación de dos hosts el fallo medio de transmisión es menor. Por el contrario, son más caras que las de difusión.

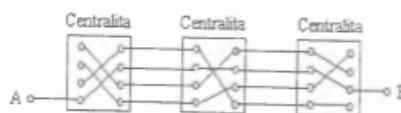
• Redes LAN, MAN y WAN:

Redes	LAN	MAN	WAN
Acrónimo	Local Area Network	Metropolitan Area Network	Wide Area Network
Coste	La más barata	Más cara que LAN.	La más cara.
Velocidad	10 Mbps - 10 Gbps	10 – 100 Gbps	57 Kbps – 20 Mbps
Rango	1 km	50 km	1000 km
Topología	<p>Bus común Ethernet (IEEE 802.3).</p> <p>Topología anillo Token Ring (IEEE 802.5).</p>	<p>Bus Dual de Cola Distribuida (DQDB).</p> 	<p>Estrella, Anillo, Árbol, Red Completa, Red de Intersección de anillos, Red Irregular.</p> <p>Dos tipos:</p> <ul style="list-style-type: none"> - Públicas: El moderador es una entidad pública o está abierta a un público general. RTC – Red Telefónica Conmutada.

			RDSI – Red Digital de Servicios Integrados. - Privadas: El moderador es una entidad corporativa y la emplea para fines propios. (SNA o DNA).
Ubicación de los ordenadores conectados a la red	En el mismo edificio.	En la misma ciudad usando módems o líneas de teléfono.	Distribuidos por el país o el continente. Conexión vía satélite o Internet (Conexiones punto a punto).
Ejemplos	Una oficina con diferentes departamentos conectados a una red.	Un banco cuyas sucursales están distribuidas por la ciudad.	Las oficinas de Google alrededor del mundo.

Las redes **WAN** también se pueden clasificar por la forma de establecer la comunicación en la red:

- a) **Conmutación de circuitos:** Empleando un camino fijo y a través de **switches** físicos. **Conversión de señal digital a analógica (por el modem).**



Para realizar la transmisión de datos a través de la RTC es necesario emplear un dispositivo especial. Las líneas telefónicas analógicas están diseñadas para la transmisión de voz, por lo que para transmitir la información digital que emplea una computadora (dígitos binarios) es necesario añadir información digital a una señal analógica que se transmite por la RTC. Esta función la realiza el dispositivo denominado módem (modulador-demodulador), que transmite y recibe información digital empleando un medio de transmisión analógico.

- b) **Conmutación de paquetes:** La información a transmitir se fragmenta en paquetes. Consta de **cabecera**, donde se incorpora información acerca de donde va dirigido el paquete y como ha de ser recompuesto el mensaje, y un campo de **datos**.



Para el establecimiento de comunicación entre emisor y receptor se emplean **circuitos virtuales**, es una analogía con el sistema telefónico de conmutación de circuitos. Los circuitos virtuales pueden ser **permanentes** o **no permanentes**. En la transmisión de paquetes de información de origen a destino se establece un camino virtual. La creación de caminos virtuales presenta más retardos que la comunicación de circuitos:

- **Congestión:** Un dispositivo que precisa de recursos software, pero hay demasiado tráfico en la red y no se le pueden proporcionar dichos recursos.
- **Saturación:** Un dispositivo de conmutación tiene una capacidad física determinada y sufre saturación cuando ya no puede realizar más conexiones.

También se emplean los **datagramas**, paquetes que contienen información acerca de su destino, pero no del camino a seguir a través de la subred. Encamina los paquetes por un camino u otro dependiendo de los recursos disponibles. Los paquetes llegan desordenados, por lo que no es un método de transmisión de datos fiable.

Arquitectura de una Red de comunicaciones hace referencia a un conjunto de protocolos perfectamente definidos e implementados que caracterizan cómo se realiza la transmisión de datos

Modelo de referencia OSI/ISO:

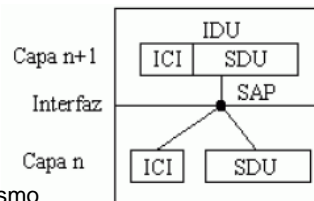
- Una capa se define cuando se necesita un **nivel diferente de abstracción**.
- Cada capa tiene una **función bien definida**.
- La **función de cada capa** se define con la **intención de crear protocolos reconocidos internacionalmente**.
- Los límites entre cada capa se eligen de forma que el **flujo** de información en las **interfaces sea mínimo**.
- El **número de capas** debe ser **elevado** para que estas sean lo más **independientes** posible y **pequeño** para que sean de **fácil manejo**.

se define en una serie de capas o niveles que interaccionan entre sí, de forma que se facilita el diseño de la red y la gestión de fallos en el funcionamiento

Servicios.

- Conjunto de funciones (primitivas de servicio) que una capa n ofrece a la capa n+1, su capa adyacente superior (comunicación vertical).
- Los puntos en los que la capa n+1 tiene acceso a los servicios de la capa n se denominan puntos de acceso al servicio (SAP).

La Capa n conversa con la capa n del otro extremo de la comunicación empleando unas normas definidas en los protocolos.



Esta comunicación horizontal entre entidades pares es virtual. La comunicación real se produce enviando información de datos y control de las capas superiores a las menores (comunicación vertical) alcanzando el nivel físico, donde la información digital se transmite empleando señales que se propagan por un medio físico

A cada una de estas capas que dialogan a un mismo nivel dentro de la arquitectura se las denomina entidades pares

SAP: Punto de acceso al servicio

IDU: Unidad de datos de la interfaz

ICI: Información de control de la interfaz

SDU: Unidad de datos del servicio

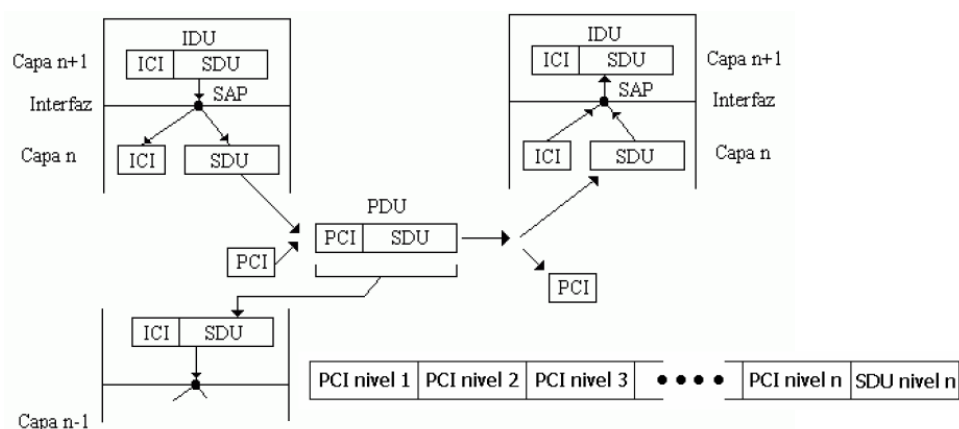
La interfaz entre capas es el elemento encargado de definir las operaciones y servicios, y de realizar la comunicación entre capas adyacentes dentro de un mismo host.

- Al conjunto de la PCI y SDU (proveniente de la capa n+1) se le denomina PDU, Unidad de Datos del Protocolo. Esta PDU será la SDU que, junto a su ICI correspondiente, se enviará a la capa n-1.

PCI es la Información de Control del Protocolo y contiene la información necesaria para poder realizar la comunicación entre las entidades pares de la capa n

Protocolos. la SDU de la capa n+1 que ha de transmitirse a la entidad par de la capa n es demasiado grande para encapsularla en una única PDU, por lo que se produce una fragmentación de la SDU en varias PDU, cada una con su correspondiente cabecera PCI. En el otro extremo se realizará la reconstrucción de la SDU original.

- Conjunto de reglas de utilización de las primitivas de servicio suministradas por el nivel inferior para la comunicación a nivel horizontal.
- **Protocolo de nivel n:** Conjunto de normas para el intercambio de PDU entre entidades pares de nivel n (comunicación horizontal).
- **Fragmentación en el protocolo de la capa n:** Mecanismo para incorporar en una PDU de tamaño limitado una SDU. La fragmentación es necesaria para que los errores provoquen reenvíos de PDUs limitadas en tamaño.
- **Comunicación horizontal y vertical en el modelo OSI:**



PDU: Unidad de datos del protocolo

PCI: Información de control del protocolo

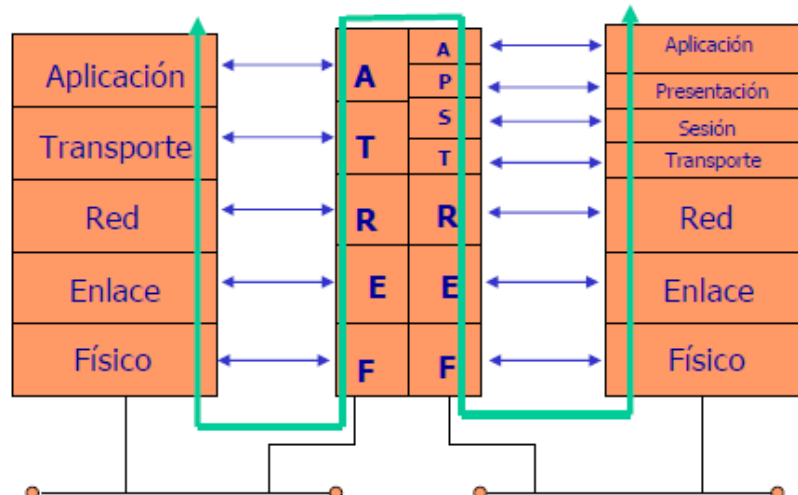
Tabla resumen Modelo OSI vs Modelo TCP/IP:

Modelo TCP/IP		Modelo OSI		Característica			PROTOCOLOS					
CAPA 4	APLICACION	CAPA 7	APLICACION	Procesos de Red a Aplicaciones			TELNET/SSH (Protocolo Emulación Terminal) FTP (Protocolo transferencia de archivos) TFTP (Protocolo trivial de transferencia de archivos) HTTP/HTTPS (Protocolo transferencia Hipertexto) SMTP (Protocolo simple de transferencia de correo) POP (Protocolo de Oficina de correos) DHCP (Protocolo configuración dinámica de Host) DNS (Sistema de resolución nombres de Dominios) SNMP (Protocolo simple administración de Redes)		DATOS			
		CAPA 6	PRESENTACION	Representación de datos								
		CAPA 5	SESION	Comunicación entre Hosts								
CAPA 3	TRANSPORTE	CAPA 4	TRANSPORTE	Conexión de Extremo a Extremo Fiabilidad de los datos			Software	TCP (orientado a la conexión/fiable) TELNET=23 / SSH=22 / FTP=21 DNS=53 / IMAP=143 HTTP = 80 / HTTPS = 443	UDP (no orientado a la conexión/no fiable) TFTP=69 / RIP=520 / DNS=53 / DHCP=67 y 68 SNMP=25 / IMAP= 143	SEGMENTOS		
CAPA 2	INTERRED (INTERNET)	CAPA 3	RED	Direccionamiento lógico y mejor ruta (b) Tabla de enrutamiento (Router)				IP		PAQUETES	ROUTER SWITCH (nivel 3)	
CAPA 1	SUBRED (RED)	CAPA 2	ENLACE DATOS	Acceso a los medios/Control errores Direccionamiento fisico (MAC/LLC) (c) Tablas direcciones, Mac, ARP STP (802.1d)/RSTP (802.1w)		LLC	802.2	Estandares: ITU, ISO, IEEE, ANSI, IAB		TRAMAS	SWITCH (nivel 2)	Misma capa cable cruzado, Capa contigua cable plano, Capa Host con Capa Router cable cruzado
		MAC										
		CAPA 1	FISICA	Ethernet, Token Ring, Otros medios Señal y Transmisión binaria (cables, conectores, voltajes, etc.) Cable par trenzado con RJ45 (T. en Estrella) Cable coaxial con BNC en T (T. en Bus)		802.3		Hardware	Ethernet	Transmisión Digital/Analógica Transmisión Sincrona/Asincrona Transmisión Serie/Paralelo Transmisión Simplex/Half-duplex/Full-duplex	IEEE 802.3 Ethernet IEEE 802.5 Token Ring IEEE 802.11 Wiffi IEEE 802.15 Bluetooth IEEE 802.16 Wimax	

Concentrador - HUB
Conmutador - Switch

Interconexión de Redes:

- a) **Gateway o pasarela:** Interconecta redes con distinta arquitectura de red.

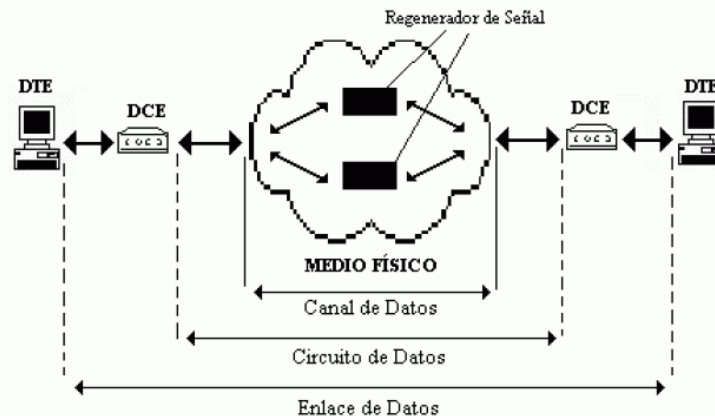


- b) **Router o encaminador:** Este dispositivo interconecta generalmente redes que presentan necesidades de encaminamiento de la información, por lo que trabaja en el nivel de red de la arquitectura.
- c) **Bridge o puente:** Este dispositivo interconecta generalmente redes teniendo en cuenta las características que presentan a nivel de enlace.

Capítulo 3:

Transmisión de señales:

- **DTE:** Equipo Terminal de Datos.
- **DCE:** Equipo de Circuito de Datos.
- **Medio de Físico:** Empleado para la transmisión de señales.
- **Regeneradores de Señal:** Estos dispositivos actúan como amplificadores y se emplean cuando las señales deben de transmitirse a distancias elevadas.



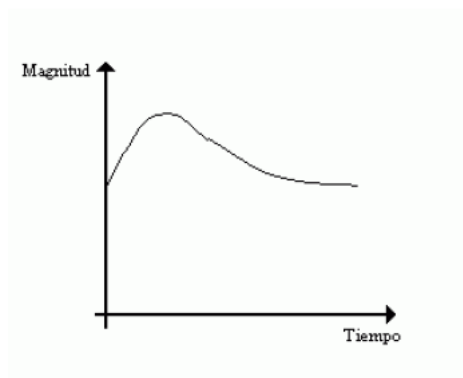
Jerarquías:

- a) **Canal de Datos:** Define una transmisión unidireccional de datos a través del medio físico. Comprende por tanto el medio físico y los regeneradores de señal.
- b) **Circuito de Datos:** Define la comunicación entre dos DCE. Esta comunicación puede comprender más de un canal de datos.
- c) **Enlace de Datos:** Define la comunicación entre dos DTE. En este nivel se consideran funciones adicionales de control de errores que implementan los DTE.

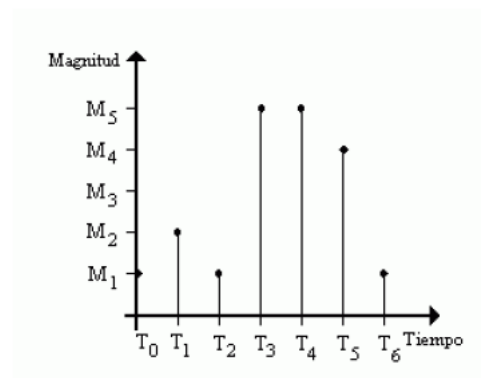
Análisis de señales con series de Forier (Ancho de Banda):

- Se entiende por **señal** la variación en el tiempo de una magnitud física.
- a) Señales **analógicas:** Cuando la magnitud física varía de forma continua a lo largo del tiempo.
 - b) Señales **digitales:** Cuando la magnitud física adquiere determinados valores en determinados instantes de tiempo, no estando definida en otros instantes.

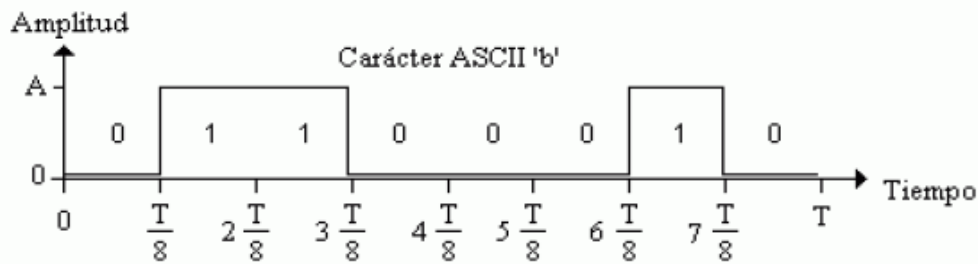
Señal analógica



Señal digital



- Señal analógica y periódica de pulsos asociada a la transmisión secuencial de un carácter ASCII.



- El **ancho de banda** de un medio físico determina cuál es el rango de frecuencias que un medio transmite produciendo un decremento en amplitud que no afecta al reconocimiento de la señal.

Velocidad de Transmisión (Teorema de Nyquist):

- **Velocidad de modulación:** Número de veces por unidad de tiempo que la magnitud física de la señal puede cambiar su valor. Si la unidad de tiempo es el segundo, la unidad de velocidad de modulación se denomina **baudio**.
- **Velocidad de transmisión:** Número de bits transmitidos por un medio por unidad de tiempo. La unidad de velocidad de transmisión comúnmente empleada es el bit por segundo (bps).
- **Nyquist:** Demostró que, si se hace pasar una señal a través de un medio con un ancho de banda (B), dicha señal puede reconstruirse a partir de las muestras tomadas con una frecuencia igual a dos veces el ancho de banda del medio ($f_m = 2B$).

Distorsión en el medio de transmisión:

- **Atenuación.** La atenuación de una señal cuando se propaga por un medio de transmisión consiste en un decremento en la amplitud de la señal original. Solución: **Ecualizadores**, amplifican de forma distinta cada componente armónica de una señal, de forma que la atenuación de la señal en el medio no impide que se recupere correctamente.
- **Ancho de banda limitado.** La limitación en el ancho de banda del medio de transmisión distorsiona las señales al eliminar componentes armónicas de la señal. Esto produce que la señal a la salida del medio físico no sea exactamente la original, al faltar información de los componentes armónicos absorbidos en el medio.
- **Distorsión de retardo.** La velocidad de propagación de una señal senoidal pura (armónico) a través de un medio físico varía con su frecuencia. Este efecto produce que cada armónico correspondiente a una señal llegue en diferentes instantes de tiempo al receptor, produciendo una distorsión en la señal. Además, según aumenta la velocidad de transmisión esta distorsión es mayor, por lo que se produce el aumento de la distancia entre dos bits consecutivos y por tanto interferencias en el valor del bit siguiente.
- **Ruido.** El ruido son aquellas perturbaciones aleatorias que están presentes en los medios de transmisión y que producen distorsiones adicionales a las señales que se propagan a través de ellos.

Tipo de Ruidos (Teorema de Shannon):

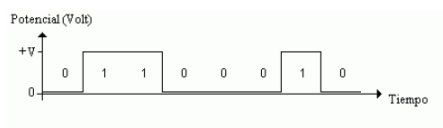
- **Razón señal a ruido** (signal to noise ratio): Expresa la relación entre la potencia de la señal propagada en el medio y la del ruido.
- **Teorema de Shannon** y se expresa como: $Vt_{max} = B * \log_2(1 + S/N)$ bps
- **Tipos de ruidos:**
 - **Ruido cruzado o diafonía (crosstalk).** Este ruido se produce por el acoplamiento entre medios de transmisión cercanos (inducción electromagnética).
 - **Autoacoplamiento.** Se produce cuando una señal de alta intensidad a la salida del DCE induce perturbaciones en una señal débil de entrada al DCE.
 - **Ruido de impulso.** Debido a la operación de aparatos que generan ruido electromagnético en las cercanías del medio de transmisión.

Capítulo 4:

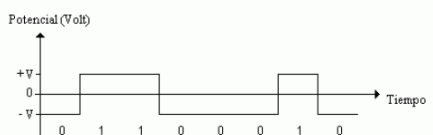
Señalización de la información (Banda Base):

- **Señal en banda base:** Señales por pulsos en medio físico analógico.
- **Codificación binaria:** Cada valor lógico de la señal de información tiene asignado un nivel de tensión eléctrica (valor de la magnitud física).

Sin retorno a 0



UNIPOLAR

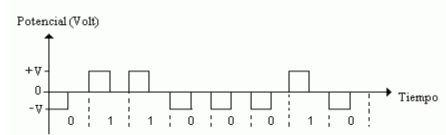


BIPOLAR

Con retorno a 0

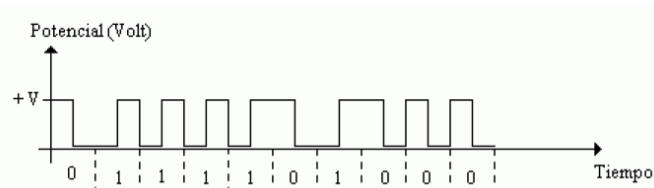


UNIPOLAR



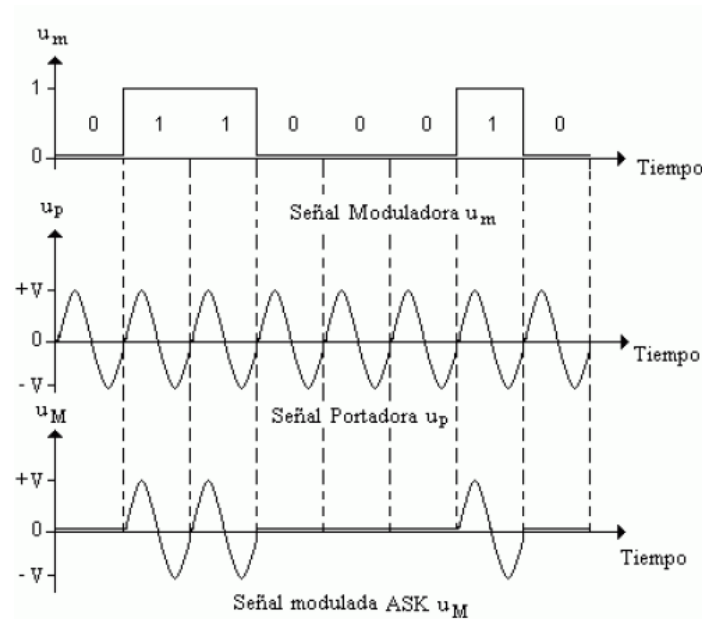
BIPOLAR

- **Codificación Manchester:** Cada valor lógico de la señal de información tiene asignado un tipo de transición en el cambio del valor de la tensión eléctrica (valor de la magnitud física). No presenta problemas de sincronización.

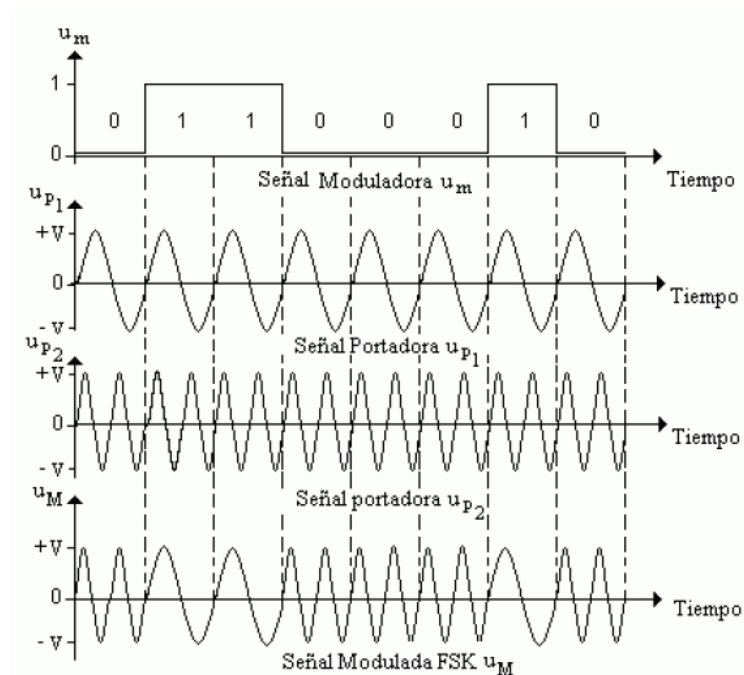


Señalización de la información (Banda Modulada):

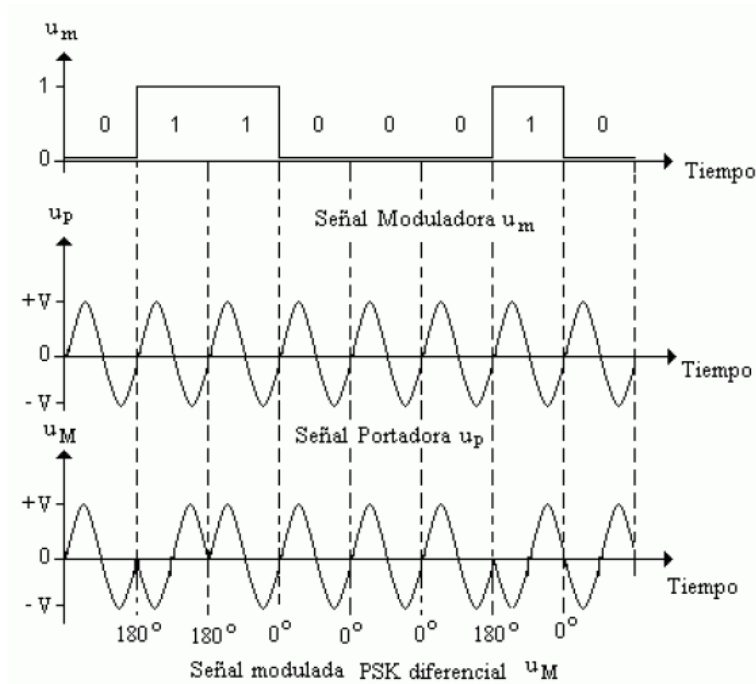
- **Señal modulada:** Incorporar información de una señal moduladora en una señal portadora que se transmite de forma adecuada por un medio de transmisión.
- **Señal moduladora:** Señal de información a transmitir. **DIGITAL** (Señal de pulsos con información binaria).
- **Señal portadora:** Señal con unas características que permite su transmisión por el medio físico. **ANALÓGICA** (Señales periódicas senoidales).
- **Modulación por cambio en amplitud (ASK):** La señal se modula cuando el valor de la señal moduladora es 1. De lo contrario (si fuera 0) se mantiene estable y constante.



- **Modulación por cambio en frecuencia (FSK):** La señal se modula (cambia de frecuencia) cuando el valor de la señal moduladora cambia de 0 a 1 o de 1 a 0.



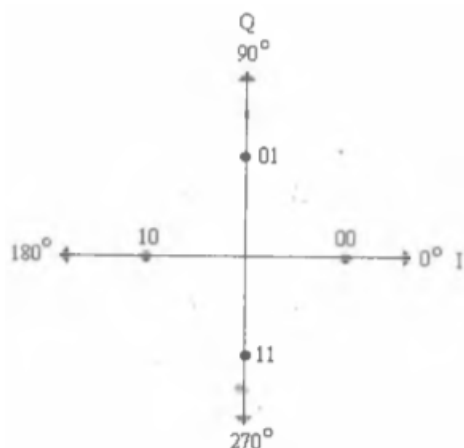
- **Modulación por cambio en fase (PSK):** La señal se modula (da 180°) cuando el valor de la señal moduladora es 1.



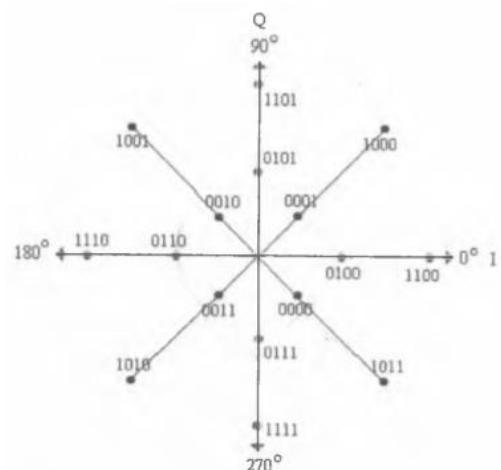
Métodos de modulación de múltiples niveles:

- Es posible conseguir un aumento en la velocidad de transmisión aumentando el número de bits (aumentando el número de niveles) que representa cada variación de la señal.
- Si se emplea como **modulación base la PSK**, el número de niveles puede aumentarse empleando un diagrama de fase. En el diagrama de fase se indica la secuencia de bits que codifica cada cambio de fase y amplitud.
- Aumentando el número de bits codificados por **cambio de fase a 2** se obtiene la denominada modulación de cambio de fase en cuadratura (**QPSK**).
- Si además del **cambio de fase a 4** se tiene en cuenta **cambios en la amplitud de la señal** portadora se obtiene modulaciones como la modulación de amplitud en cuadratura (**QAM**).

QPSK

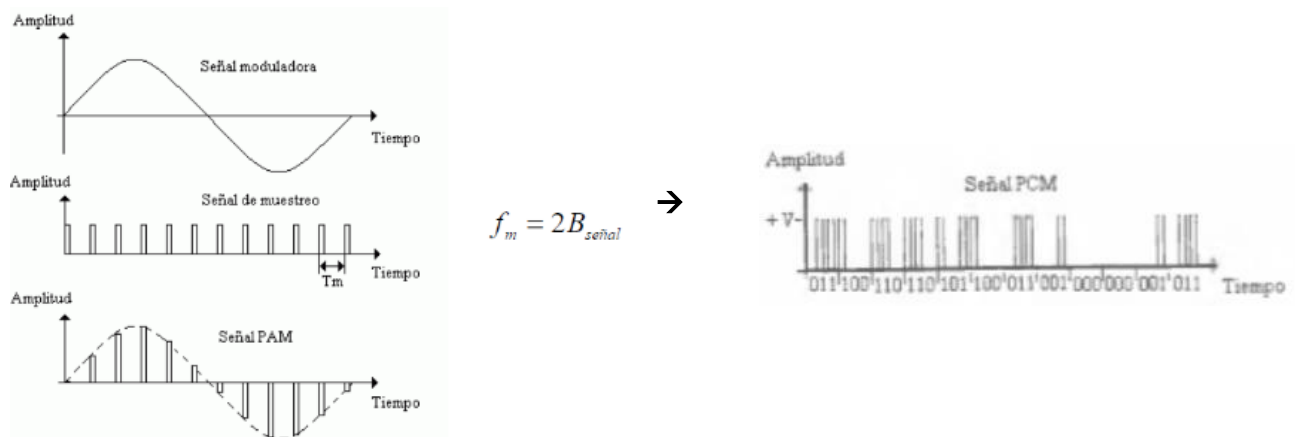


QAM



Modulación Digital.

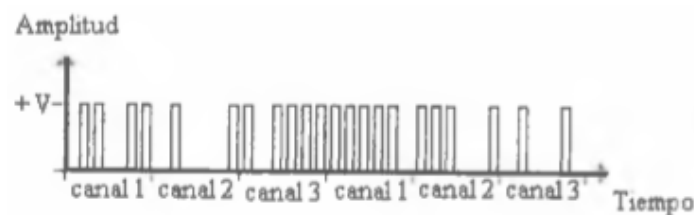
- **Modulación por código de pulsos (PCM):** La señal se modula de una señal analógica en una secuencia de bits (señal digital). Los niveles de **cuantificación** digital son linealmente uniformes.



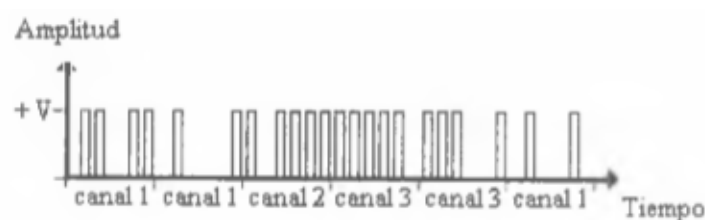
Señal Pulso Analógico Modulada (PAM)

Multiplexión.

- El **mecanismo** permite establecer varios canales de datos en un único circuito de datos, uniendo varios canales de velocidad moderada en un canal de alta velocidad.
- **Multiplexión por división de frecuencias (FDM):** Se emplea en líneas de transmisión analógicas, como son las líneas telefónicas. Su funcionamiento se basa en repartir el ancho de banda del medio de transmisión en ventanas de frecuencia donde se incorporan los espectros de las señales a transmitir, de forma que pueden enviarse simultáneamente.
- **Multiplexión por división en el tiempo (TDM):** Asignar celdas de tiempo para la transmisión de información de cada canal.
 - a) **Multiplexión síncrona.** Los fragmentos de tiempo asociados a cada canal son fijos y asignados antes de iniciar la transmisión.

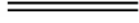

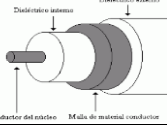
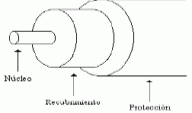
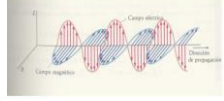



- b) **Multiplexión asíncrona/estadística (STDM).** Los fragmentos de tiempo asociados a cada canal se asignan dinámicamente en base a la demanda, mejorando el rendimiento.



Capítulo 5:

Medios de transmisión:

Nombre	Cable par paralelo	Cable par trenzado no blindado (UTP)	Cable coaxial	Fibra óptica	Ondas electromagnéticas
Imagen					
Distancia máxima	50 m	Categoría 3, Categoría 5 y Categoría 6: 100 m	100 m	Dispositivo regenerador de señal en el punto de corte.	Varía dependiendo del medio.
Velocidad	20 Kbps	Categoría 3: 30 Mbps Categoría 5: 100 Mbps Categoría 6: 1000 Mbps	1000 Mbps	Multimodo 20 MHz/Km Índice gradual 500 - 1000 MHz/Km Monomodo 1 - 10 GHz/Km	2.4 y 5 GHz 600 Mbps
Características	Comunicaciones DTE - DCE	Reduce el ruido cruzado o diafonía  Existen mejoras en el STP (reduce más el ruido y tiene una mayor velocidad)	La malla conductora evita las interferencias de campos eléctricos externos al cable y <u>elimina</u> el ruido de impulso. Cable coaxial 50 Ω: Transmisión en banda <u>base</u> (Manchester). Redes LAN (sustituido por pares trenzados). -Velocidad de 10 Mbps a distancia de 100 m para cable coaxial fino. -Velocidad de 10 Mbps a distancia de 500 m para cable coaxial grueso.	Núcleo de cristal de sílice rodeado de un recubrimiento de silicona. Dispone de una capa externa como protección hecha de poliuretano. Medio que permite el <u>confinamiento</u> y <u>propagación</u> de un <u>haz de luz</u> . La propagación de la luz entre dos medios distintos distorsiona la trayectoria del haz, produciéndose una refracción o reflexión. <u>No se produce ni dispersión ni ruido.</u> A) Fibra multimodo o de índice de salto: Existen múltiples haces que se propagan en la fibra, desfasándose temporalmente debido a los diferentes recorridos ópticos.	La radiación electromagnética es un mecanismo de transmisión de energía que presenta las propiedades de una <u>onda</u> . Esta onda es susceptible de incorporar información empleando mecanismos de modulación (ASK, PSK, FSK). El espectro de radiocomunicación es el conjunto de frecuencias de radiación electromagnética que se han definido para incorporar información y se emplean en los sistemas de comunicaciones. Esta elección es por diversos

			Cable coaxial 75 Ω: Transmisión en banda <u>modulada</u> . <u>Multiplexión</u> en frecuencia de múltiples canales (transmisión broadband - 300 MHz). (Televisión analógica/digital por cable).	B) Fibra de índice gradual: El índice de refracción variable en el núcleo permite compensar el efecto de la dispersión <u>intermodal</u> (a mayor velocidad, esto aumenta). C) Fibra monomodo: Un núcleo de diámetro muy reducido permite la propagación de un único haz en paralelo al eje de la fibra. No existe dispersión intermodal, pero si dispersión <u>intramodal</u> .	motivos de salud, energéticos y propiedades de propagación.
--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------

Transmisión vía satélite:

- El rango de frecuencias empleado está entre **4 - 6 GHz**, que en la **actualidad** está saturado, y se ha **ampliado** al uso de la banda **12-14 GHz**.
- Los sistemas de comunicación en los satélites se integran en dispositivos individuales denominados **transponders**. Estos elementos consisten en un **sistema emisor/receptor** que emplea un ancho de banda y rango de frecuencias determinado, de forma que cada satélite dispone de varios transponders **que no se solapan** en el espectro frecuencial.

Capítulo 6:

Función genérica del nivel de enlace:

- Comunicación libre de errores en un medio físico.

Servicios del nivel de enlace:

- **Servicio sin conexión y sin reconocimiento.** Se envían tramas de información independientes a la máquina de destino sin pedir que se confirme que han llegado o no. No se establecen conexiones entre la estación origen y destino, pues al enviar tramas de datos independientes se consigue una transmisión más rápida. Tasa de errores baja en el medio físico o en algunas aplicaciones.
- **Servicio sin conexión y con reconocimiento.** Por cada trama de datos independiente que es recibida por una estación receptora, esta envía una trama de asentimiento confirmando la recepción de la trama de datos al emisor. Se emplea, por tanto, cuando el nivel físico presenta una tasa de error no despreciable.

- **Servicio con conexión y con reconocimiento.** Se envían cada una de las tramas de datos numeradas, que serán confirmadas por el receptor y, en caso de que alguna sufra errores en la transmisión, se realizará el reenvío de esta. El servicio conectado es **más fiable**.

Funciones del nivel de enlace:

- **Delimitación de tramas:** Identificación del inicio y fin de un paquete.



Formato de la trama Ethernet

Dir. Destino	Dir. Fuente	Tipo	datos	CRC
6	6	2	46 - 1500	4

- **Direccionamiento:** Identificación de los extremos de la comunicación en un medio físico.

El objetivo es identificar los elementos que intercambian tramas de nivel de enlace en un medio físico. Para ello, se asignan secuencias de bits únicas a cada estación.

- **Implícito:** No es necesario especificar las estaciones origen y destino que intercambian tramas.
Ej: Línea punto a punto.
- **Explícito:** Es necesario especificar las estaciones origen y destino que intercambian tramas.
Ej: Ethernet.

- **Control de errores:** Asegura una transmisión sin errores debidos al medio físico.

○ Detección y corrección de errores:

- **Secuencia de Verificación de Trama (FCS o SVT):** Conjunto reducido de datos que suele añadirse en la cola de un paquete de enlace. Dependiendo del tipo de información en la FCS se distingue entre:

A) Códigos de detección de error.

B) Códigos de corrección de error.

En A) solo permite detectar si el paquete tiene algún bit erróneo, en B) el receptor puede identificar el problema y corregirlo. Este método no se emplea actualmente.

○ Métodos de detección de errores:

- **Detección de errores por paridad de bits de datos:** Permiten detectar si en el paquete hay errores en un número impar de bits. Incorporan mucha información redundante, en comparación con otros sistemas.
- **Detección de errores por Códigos de Redundancia Cíclica (CRC):** Asocia un bloque de datos a un polinomio en x, determinando la SVT mediante operaciones y propiedades de polinomios. La elección del polinomio generador se realiza para cumplir con las propiedades de detección de errores más adecuadas.

- **Control del flujo:** Control del flujo de tramas entre emisor y receptor para **evitar saturaciones**, reenvíos incorrectos, etc.

Capítulo 7:

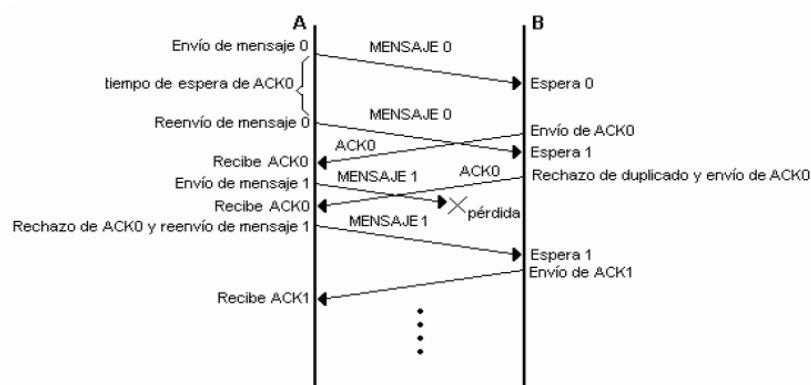
Control del flujo:

- **Controlar el envío y recepción correcto** de los paquetes de nivel enlace.
- **Controlar la sincronización** del emisor y receptor de datos.
- **Evitar congestiones** en el envío de información del emisor al receptor.

Protocolos:

- **Protocolos de parada y espera:** El control del flujo se establece en que el emisor debe esperar a una confirmación por parte del receptor por cada bloque de datos enviado para poder continuar la transmisión.

Presenta 2 problemas, duplicación (Solución: Numeración de tramas) y pérdida de la sincronización (Solución: Asentimientos).

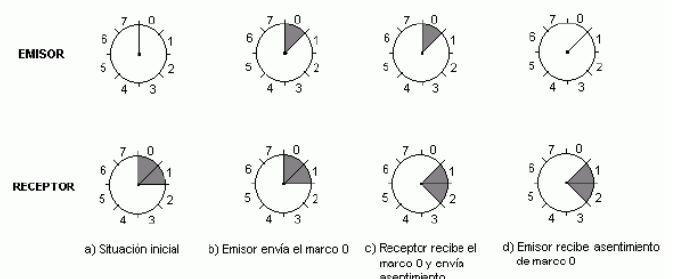


- **Protocolos de ventana deslizante:** Mejorar el aprovechamiento del canal de comunicación enviando datos, aunque no se haya recibido el ACK de los datos.
 - **Ventana del emisor:** Conjunto de secuencias de numeración de los paquetes que el emisor ha transmitido y de los que no ha recibido su ACK correspondiente. Debe permitir como MÍNIMO transmitir paquetes hasta que llega el primer ACK de datos.
 - **Ventana del receptor:** Conjunto de secuencias de numeración de los paquetes que el receptor espera recibir y de los que enviará ACK. No debe permitir repeticiones de secuencia en una rotación completa.
 - **Tamaño de ventana del emisor/receptor:** Número de secuencias en la ventana del emisor/receptor.

Funcionamiento:

Cada vez que el emisor envía un paquete de datos se añade su secuencia a la ventana del emisor. Existirá por tanto, un número máximo de secuencias en la ventana del emisor. El receptor espera paquetes de datos cuya secuencia esté en la ventana del receptor. Cuando se recibe un paquete con secuencia dentro de la ventana del receptor, se envía un ACK de la secuencia al emisor.

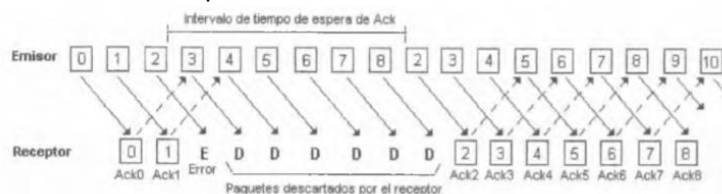
Número de secuencias: 8 (0-7)
Tamaño de la ventana del emisor: 1
Tamaño de la ventana del receptor: 2



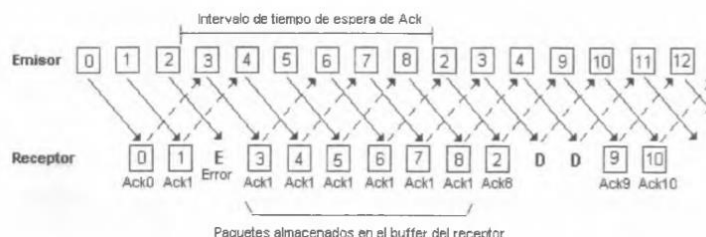
El tamaño de la ventana del emisor **VARÍA** y la del receptor es **CONSTANTE**

Tipos de Ventanas deslizantes:

- **Protocolo de ventana deslizante de 1 bit:** Este protocolo se caracteriza por que la numeración de tramas y ACK se realiza empleando un único bit, por lo que las secuencias enviadas estarán numeradas como 0-1-0-1... El tamaño de la ventana del emisor y receptor es el mismo y tiene valor 1, por lo que es equivalente al protocolo de parada y espera con incorporación.
- **Protocolo de ventana deslizante de envío continuo con repetición no selectiva:** El tamaño de la ventana del emisor limitado a 1 impide un mejor aprovechamiento del medio físico para el envío de datos, que está inactivo hasta la llegada del ACK del receptor.



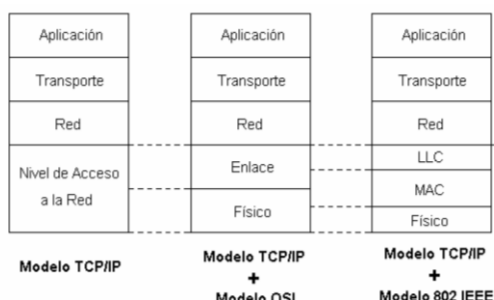
- **Protocolo de ventana deslizante de envío continuo con repetición selectiva:** Los paquetes no han de recibirse en orden al aceptar el receptor más de un número de secuencia. Se hace preciso por tanto de la existencia de un buffer en el receptor donde las tramas son almacenadas temporalmente y ordenadas antes de ser enviadas al nivel de red. Cuando se produce un error, el receptor almacena tramas dentro de su ventana y espera la secuencia inicial de la misma. Todas las tramas que lleguen a continuación y que no estén en la ventana del receptor serán rechazadas. Cuando llega la trama inicial de la ventana, el receptor envía el ACK de la última trama en el buffer.



Tema 4.1:

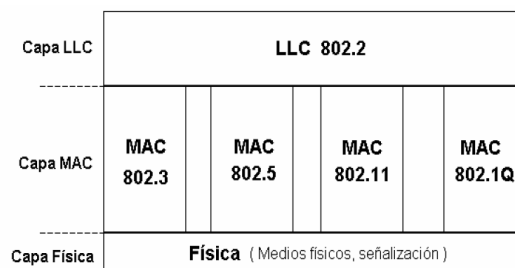
Redes LAN. Normas IEEE 802.x:

- El IEEE desarrolla una normativa para el intercambio de información en una LAN desarrollando una arquitectura de 3 niveles (LLC, MAC y físico). Una red LAN puede intercambiar información empleando los niveles de enlace y físico. La normativa del IEEE se denomina **Modelo de Referencia IEEE 802**.
- Incorporación del modelo del IEEE en el modelo TCP/IP:**
- Arquitectura IEEE 802:**



LLC: Control del Enlace Lógico. Funcionalidad de control del flujo y de errores.

MAC: Control de Acceso al Medio. Funcionalidades de reparto del medio físico, direccionamiento físico, etc.



IEEE 802.2: Protocolo de Control del Enlace Lógico (LLC)

IEEE 802.3: Ethernet (CSMA/CD)

IEEE 802.11x: LAN Inalámbrica

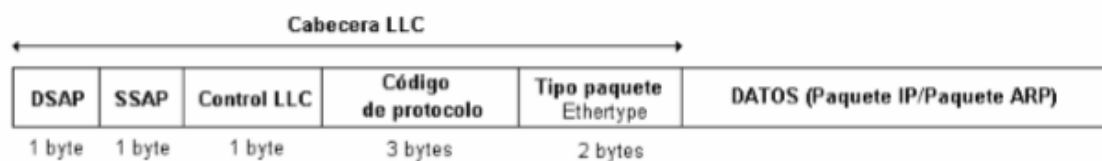
IEEE 802.5: Token Ring (Anillo con testigo)

IEEE 802.1Q: LAN Virtual (VLAN)

Protocolo IEEE 802.2 LLC:

- El **protocolo LLC** (Protocolo de Control del Enlace Lógico) se diseñó para proporcionar un conjunto de funcionalidades asociadas a la capa de enlace del modelo OSI. Se basó en el protocolo **HDLC**, es decir 3 mecanismos para el envío de paquetes del nivel de red:
 - **Servicio no orientado a conexión y sin confirmación:** Sin control de errores ni de flujo, pero muy rápido.
 - **Servicio orientado a conexión:** Servicio con control de errores y de flujo, más lento.
 - **Servicio no orientado a conexión con confirmación:** Servicio con confirmación de paquetes.

Formato de paquete LLC para redes TCP/IP:



- **DSAP:** Punto de Acceso al Servicio de Destino. En el caso de arquitectura TCP/IP tiene asociado el valor 170.
- **SSAP:** Punto de Acceso al Servicio de Origen. En el caso de arquitectura TCP/IP tiene asociado el valor 170.
- **Control LLC:** En el caso de arquitectura TCP/IP tiene asociado el valor 3.
- **Código de protocolo:** Indica qué tipo de información viene a continuación. En el caso de la arquitectura TCP/IP tiene asociado el valor 0.
- **Tipo paquete:** Los paquetes de datos IP tienen asociados el valor 2048 (0x0800), y los paquetes ARP el valor 2054 (0x0806).

Tema 4.2:

Ethernet:

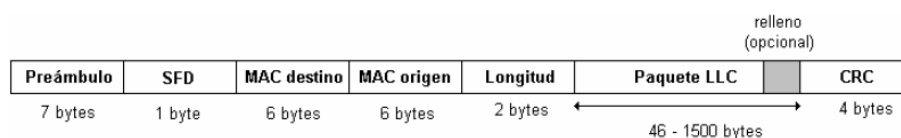
- Una red Ethernet se caracteriza por emplear un **medio físico compartido** (cable coaxial, cable par trenzado o fibra óptica) entre todas las estaciones con topología de **bus**. Son **semiduplex** y emplean un mecanismo denominado **CSMA/CD** (bus) para el reparto del medio físico.
- **Velocidad – Señalización - Medio físico:**
 - **10Base2:** Significa Red Ethernet (una de las primeras versiones) a **10 Mbps** a distancias de **185 metros**, señalización en banda base (**Manchester**) y medio físico cable **coaxial fino**.
 - **Velocidad:** 10 (Mbps), 100 (Mbps), 1000 (Mbps), 10 (Gbps).
 - **Señalización:** Base (banda **base**) o Broad (banda **modulada**).

- **Medio físico:** T (cable UTP), C (cable STP), F (fibra óptica), X (soporte para varios medios físicos).
- **10Base5** emplea cable **coaxial grueso**, permitiendo una velocidad de **10 Mbps** a distancias de hasta **500 metros**.
- **10Base2** y **10Base5** desaparecen del mercado con la introducción de los cables UTP (más tolerancia a fallos, facilidad de implantación y mejores prestaciones).

Formato de paquete IEEE 802.3:

Las redes LAN 802.3 conforman una red con buen rendimiento para bajo tráfico. Establece un formato de paquete donde se especifica la cabecera MAC:

- **SFD:** Delimitador de inicio de trama.
- **MAC destino/origen:** Identificador de 48 bits para cada equipo.
- **Longitud:** Tamaño del campo de datos del paquete (máximo 1500).
- **CRC:** Código de Redundancia Cíclica de 32 bits para detección de errores.



Formato de paquete Ethernet II:

Las redes Ethernet de Digital/Intel/Xerox (**Ethernet DIX**) emplean un **formato de paquete distinto**. Este formato, denominado Ethernet II, no emplea la capa LLC y permite la introducción del datagrama IP en el paquete de nivel MAC.

CSMA/CD – Acceso al Medio con Detección de Portadora y de Colisión:

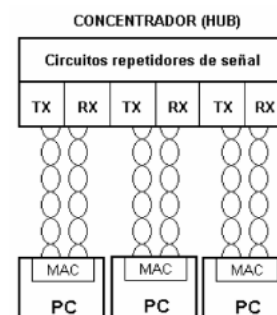
Comprueba si el **medio físico** está libre antes de transmitir un paquete de datos. El esquema de funcionamiento es siempre **semidúplex**:

- **Problemas:** **Colisión** por comprobación simultánea del bus por dos o más estaciones.
- **Solución:** En cada intento se **espera** un **número aleatorio** de veces antes de volver a intentar emitir una señal.

Conmutación y puentes:

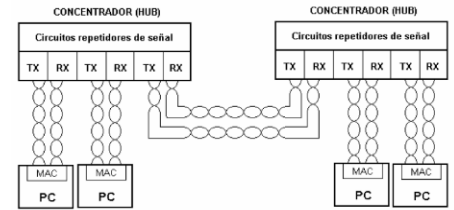
• Concentrador Ethernet (Hub):

- La **red 10BaseT** surge con la introducción de los cables pares trenzados no blindados (UTP).
- Un cable UTP comercial está formado por 4 pares de hilos trenzados.
- 10BaseT emplea el **cable de categoría 3** (30 MHz) con **codificación Manchester**, alcanzando sin problemas la **velocidad de 10 Mbps a distancias de 100 metros**.
- Utiliza una **topología en estrella**.
- El elemento central se denomina concentrador o hub.
- Las colisiones se detectan cuando se recibe una señal por el par de recepción al mismo tiempo que se transmite una trama.
- La **detección de problemas** en el cableado es **más fácil** que con cable coaxial.
- La **distancia máxima** entre equipo y concentrador debe ser **inferior a 100 m**.
- La red Ethernet **puede crecer** en tamaño interconectando concentradores con cables UTP cruzados (**repetidores**).



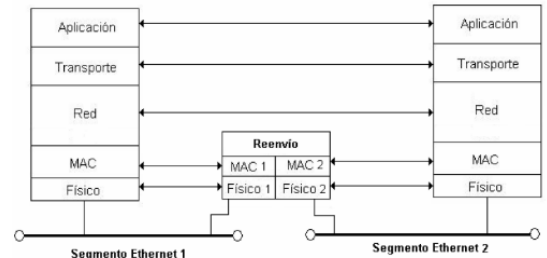
- **Repetidores (hubs en cascada):**

- La **conexión de concentradores en cascada** permite el aumento en el tamaño físico de la red Ethernet.
- **Dominio de colisión:** Conjunto de dispositivos en una red que pueden colisionar al transmitir simultáneamente.
- **Inconveniente del hub:** Aumenta la probabilidad de colisiones al ser mayor el dominio de colisión.



- **Bridges (puente):**

- Un puente es un **dispositivo de interconexión** entre dos o más segmentos Ethernet que analiza la cabecera MAC de los paquetes para determinar si hay que reenviarlos o no de un segmento a otro.
- El puente **divide la red** en segmentos de colisión independientes, por lo que las **LAN interconectadas** con puentes **no tienen limitación** de extensión física al crecer.



- **Puentes Transparentes:**

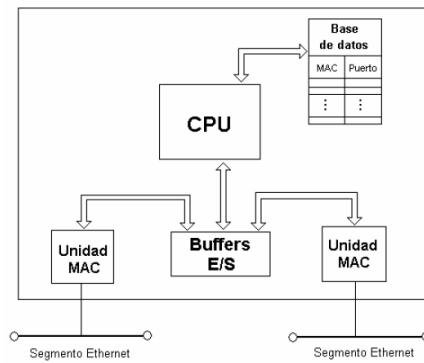
- Los puentes transparentes son aquellos puentes en los que la **decisión** de cómo los paquetes se intercambian entre segmentos **la toman ellos**. Los equipos no conocen la estructura de la red.
- Modo de **reenvío**:

Se comprueba la dirección MAC de destino de cada paquete Ethernet que llega a un puerto.

- Si la dirección MAC de destino **se encuentra** en la tabla de reenvío, el puente reenvía el paquete al puerto asociado, siempre que el puerto asociado sea distinto del puerto por donde ha llegado el paquete.
- Si la dirección MAC de destino **no existe** en la tabla de reenvío, el paquete se reenvía a todos los puertos excepto por el que se recibió.

En los paquetes con dirección de destino, la dirección de broadcast se reenvía a todos los puertos, excepto al puerto por el que se recibió el paquete de difusión.

- Modo de **aprendizaje**:
 - Se comprueba la dirección MAC de origen en cada paquete Ethernet recibido en un puerto.
 - Si la dirección MAC de origen no se encuentra en la tabla de reenvío, el puente crea una entrada con la dirección MAC de origen y el puerto donde se ha recibido.
 - Durante el proceso de aprendizaje, dado que no se conocen las direcciones MAC de los equipos, la mayor parte de los paquetes son reenviados por todos los puertos, por lo que los demás **puentes aprenderán información**. A este fenómeno se le conoce como **inundación**.
 - Si el **temporizador alcanza** un determinado valor **máximo**, la **entrada** de la tabla de reenvío **se elimina**. De esta forma, las tablas de los puentes se ajustan a cambios en la estructura de la red.
 - Cada entrada en la tabla de reenvío de un puente tiene asociado un temporizador que mide el tiempo desde que se creó la entrada en la tabla.
 - Si se recibe un paquete con una dirección MAC de origen por el puerto que se indica en la tabla de reenvío, el temporizador se inicializa a cero.
 - El modo de aprendizaje requiere que la LAN con puentes tenga una estructura de árbol simple, es decir, árbol de expansión.



CPU: Unidad de control de funcionamiento del puente (reenvío de paquetes y aprendizaje)

Buffers E/S: Unidad de almacenamiento de tramas en proceso (lectura/envío). FIFO.

Base de datos: Tabla de asociación de direcciones MAC con números de puerto (**tabla de reenvío**).

○ El algoritmo Spanning Tree:

- Define un **protocolo de comunicación entre puentes** que consiga una estructura de **LANs** interconectadas por puentes **sin** existencia de **bucles**.
- El algoritmo elige un puente, identificador más bajo, que será la raíz de la estructura de árbol (**puente raíz**).
- En cada puente se determina un coste RPC (número de redes intermedias, velocidad de transmisión) desde cada puerto al puente raíz. Al puerto con **menor coste** se le denomina **puerto raíz** del puente.
- En cada segmento se elige un puerto designado. El puerto designado de un segmento es el puerto con menor valor de RPC que esté conectado al mismo.
- Finalmente, **se activan todos los puertos raíz designados de la red**, determinando una estructura de árbol.

● Ethernet Conmutada:

Cada puerto se conecta a un equipo en vez de a un segmento de red. Estos dispositivos se denominan **conmutadores** o **switches**. Existe Ethernet mixta de concentradores/conmutadores.

- **Modo full-duplex:** No existen colisiones (CSMA/CD no activo). Transmisión y recepción simultánea.
- **Modo half-duplex:** Permite la conexión de equipos con CSMA/CD (concentrador 10BaseT).

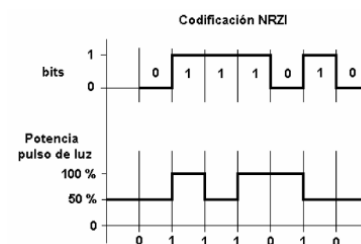
Fast Ethernet (IEEE 802.3u):

- Funcionan con **conmutadores**, permitiendo el modo de trabajo **half-duplex** y **full-duplex**.
- Si se **emplea 100 Mbps en CSMA/CD** existe el problema del **tamaño** de paquete **mínimo** para la transmisión.
- Subcapas para el nivel físico:
 - **Subcapa de convergencia:** Convierte el flujo de bits de la capa MAC en grupos de 4 bits para su envío a la subcapa PMD.
 - **Subcapa dependiente del medio físico:** Transmite cada grupo de 4 bits con el mecanismo de codificación adecuado a cada tipo de medio físico.
- **100BaseX:**
 - La normativa 100BaseX se desarrolló para cables **UTP categoría 5**, **STP** y **fibra óptica**.
 - El principal **problema de la transmisión a alta velocidad** es la **sincronización emisor-receptor** al transmitir la secuencia de bits.

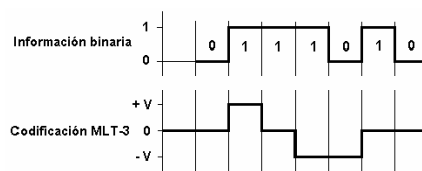
- Para introducir siempre información de **sincronización** en el flujo de bits, 100BaseX introduce una **codificación 4B/5B**.

- Cada símbolo de **5 bits** se convierte en **pulsos luminosos** empleando **codificación NRZI**.

- Emplea **fibra óptica multimodo** y permite alcanzar distancias de hasta **400 m** entre un equipo y el conmutador.



- **100BaseTX**: emplea la normativa 100BaseX de codificación 4B/5B sobre cable UTP categoría 5 (máximo **100m**). Cada símbolo de **5 bits** se convierte en **pulsos eléctricos** empleando la **codificación MLT-3**.



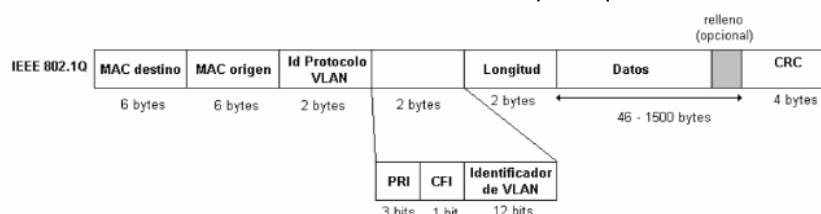
Gigabit Ethernet (IEEE 802.3z):

- Funcionan con **conmutadores**, permitiendo el modo de trabajo **half-dúplex** y **full-dúplex**.
- **1000BaseT**: Alcanzar con **cable UTP categoría 5** velocidades de **1 Gbps** en modo **full-dúplex** es **complejo** y **costoso**. Permite alcanzar distancias de **100 m** empleando los cuatro pares de hilos para transmitir y recibir simultáneamente (cancelación de eco).
- **1000BaseX**: La transmisión de datos a **1 Gbps** por **fibra óptica** es **menos compleja** debido al **enorme ancho de banda** de la fibra. Los bits del paquete Ethernet son modificados con un **codificador 8B/10B**, introduciendo información de sincronización para el receptor. La señal codificada puede transmitirse por fibra óptica o mediante cable **STP** (distancia máxima **25 m**).
- **10 Gigabit Ethernet (802.3ae)**: Funcionan con conmutadores permitiendo solamente el modo de trabajo **full-dúplex** (no existe CSMA/CD). Emplea en general la fibra óptica como medio de transmisión. Empleando **fibra óptica multimodo** se alcanzan distancias de hasta **300 m**, pero con **monomodo** se consiguen hasta **40 Km**.
- **2.5GBaseT – 5GBaseT (802.3bz)**: Estas normativas están pensadas para ser empleadas con cable par trenzado (UTP) de **categoría 5e** (2.5 Gbps) y **categoría 6** (5 Gbps) y distancias hasta **100 m**. Su **objetivo** es permitir conexiones de **puntos de acceso Wi-Fi** de la norma 802.11ac.

IEEE 802.1Q:

- Normativa para poder **dividir un conmutador en varios dominios de difusión distintos**.
- **Redes de Área Local Virtuales (VLAN)**: Cada dominio de difusión independiente.

El **funcionamiento** de un conmutador VLAN es **similar al de un puente**, disponiendo de una **tabla de reenvío**. Cada VLAN tiene asociada una **dirección** de red IP diferente para que **ARP** funcione.

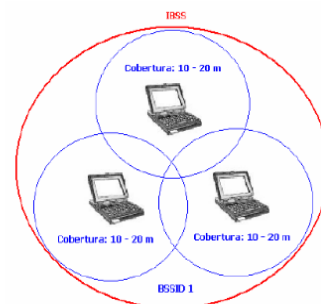


- Se emplea cuando se **interconectan** conmutadores **VLAN entre sí** o un **router a** un conmutador **VLAN**.
- Un conmutador VLAN **maneja** de **diferente** forma los enlaces de acceso y los enlaces troncales:
 - En los **enlaces de acceso** los paquetes tienen el formato del **IEEE 802.3**.
 - En los **enlaces troncales** los paquetes tienen el formato del **IEEE 802.1Q**. Los conmutadores VLAN emplean un protocolo denominado **GVRP** (GARP VLAN **R**egistration Protocol).

IEEE 802.11x.

- Red **LAN inalámbrica**: Red de área local que emplea ondas electromagnéticas como soporte físico para la comunicación de datos.
 - **BSS** (Basic Service Set): Conjunto de servicio básico. Grupo de estaciones que se comunican entre ellas.
 - **SSID** (Service Set Identifier): Identificador de un BSS. Cadena de 32 caracteres máximo.
 - **BSSID** (Basic Service Set Identifier): SSID en redes **ad-hoc**. (MAC)
 - **ESSID** (Extended Service Set Identifier): SSID en redes de **infraestructura**.
- **Normativas** de comunicación inalámbrica.
 - Tecnologías en las que destaca el IEEE:
 - **IEEE 802.11b**: Empleando una señal portadora de **2.4 GHz**. Esta frecuencia está declarada para su uso libre, por lo que pueden existir interferencias con otros dispositivos del mercado.
 - **IEEE 802.11g**: Empleando una señal portadora de **2.4 GHz**. Alcanza velocidades de hasta 54 Mbps.
 - **IEEE 802.11n**: Permite emplear la portadora de **2.4 GHz** y la de **5 GHz** (19 canales), consiguiendo velocidades de hasta 600 Mbps.
 - **IEEE 802.11ac**: Emplea solamente la portadora de **5 GHz** (19 canales) y varias antenas, consiguiendo velocidades de hasta 1.3 Gbps.
 - La señal de **2.4 GHz** llega a **más distancia** que la de **5 GHz** a pesar de que esta tiene **más ancho de banda**.
 - La **velocidad de transmisión con wireless no es fija**, le afecta el ruido del entorno de trabajo.
- **Características de acceso al medio**:
 - La elevada tasa de error en el medio introduce dos necesidades:
 - **Tamaño de paquete más pequeño**, pues los errores provocarán reenvíos más pequeños de datos.
 - **Protocolo MAC 802.11 confirmado**. Debido a la **elevada tasa de error**, es necesario que el protocolo de control de acceso al medio sea capaz de **confirmar los paquetes transmitidos**.

Red Inalámbrica ad-hoc



- El protocolo MAC del 802.11 distingue entre **dos modos de funcionamiento** para el uso del medio físico:
 - **DCF** (Función de coordinación distribuida):
 - Empleadas en **wireless** de **infraestructura** y **ad-hoc**.
 - Cada estación compite por el uso del medio físico. El mecanismo de reparto empleado es el **CSMA/CA**.
 - Para **evitar** el **problema** de la **estación oculta** (un AP detecta dos estaciones, pero las estaciones no se detectan entre ellas) se introduce un **mecanismo de reserva de la red**.
 - **PCF** (Función de coordinación centralizada):
 - Empleadas en wireless de infraestructura, donde el **AP controla** el acceso al medio compartido.
 - Este modo de funcionamiento está definido **solo** para las redes de **infraestructura**, pues **precisa** de la existencia de un **punto de acceso** (AP).
 - Cuando existe un AP todas las comunicaciones se realizan a través de él, es decir, si una estación quiere transmitir un paquete a otra estación, se enviará la información al AP y este lo reenviará a la estación destino.
 - **Periodo de no colisión:** En el periodo de no colisión, el AP envía a una estación un paquete solicitando que le envíe un bloque de datos. Cuando el bloque de datos es recibido por el AP, envía otra solicitud a otra estación.

Seguridad en redes Wi-Fi:

- **Wi-Fi Alliance:** Asociación de fabricantes de tecnología de red inalámbrica basada en la norma IEEE 802.11x.
- **Principios de seguridad:**
 - **Autenticación:** La estación cliente debe identificarse como un usuario autorizado de la red Wi-Fi.
 - **Autenticación y cifrado WEP** (Wired Equivalent Privacy): Fue el **primer protocolo de encriptación** empleado en el estándar IEEE 802.11x. El **funcionamiento** de WEP está basado en el conocimiento de **una misma clave secreta** por parte de la **estación** y el **AP** (**PSK** – Pre-Shared Key). Era el router el que mandaba la codificación al cliente.
 - **Autenticación y cifrado WPA:** La principal vulnerabilidad de WEP es la capacidad de obtener la clave de cifrado. Así, WPA mantiene el **mismo algoritmo de cifrado** de WEP (RC4), **pero introduce** el mecanismo **TKIP** (Temporal Key Integrity Protocol) que **modifica** la **clave** de cifrado entre el cliente y el AP **cada cierto tiempo**, además de introducir un mecanismo de verificación de la integridad de los paquetes cifrados.
 - **WPA–Personal** o **WPA-PSK:** En este mecanismo, cliente y AP disponen de una clave de acceso prefijada para permitir el acceso a la red inalámbrica (mismo mecanismo de WEP). La clave **PSK inicial** es **modificada posteriormente** en el cifrado **al emplear TKIP**.
 - **WPA–Enterprise:** En este mecanismo, cada **cliente autentica** su **acceso** al AP **empleando** un **servidor** de autenticación (**RADIUS**).

- **Integridad de la información:** La información debe transmitirse **cifrada para evitar espías** (sniffers).
 - **EAP/TLS:** Autenticación basada en un **certificado de servidor y cliente**.
 - **EAP/TTLS o PEAP:** Autenticación basada en un **certificado de servidor**. El cliente se valida con un **nombre de usuario y contraseña** en un **servidor RADIUS**.
 - **LEAP** (Lightweight EAP): Autenticación propietaria de Cisco Systems y que **no emplea certificados** de seguridad. La **autenticación** de un cliente se realiza **empleando** alguno de los **mecanismos de autenticación** que soporte un **servidor RADIUS** donde se almacenan los usuarios autorizados.
 - **WPA2:**
 - **Introduce un paradigma de seguridad Wi-Fi, basado en** toda la tecnología desarrollada para **WPA** y emplea **LEAP** como mecanismo de autenticación.
 - No introduce variaciones en los mecanismos de autenticación empleados en WPA (se denominan WPA2-Personal y WPA2-Enterprise), pero sí permite **mejorar la seguridad** del cifrado.
 - Permite **emplear**, además de **TKIP**, otro mecanismo de cifrado denominado **AES** (Advanced Encryption Standard), que es un estándar de cifrado y en la actualidad no se ha roto, por tanto es el **más recomendable** para accesos Wi-Fi, y no utiliza un vector de inicialización.

Tema 5:

Funcionalidades del Nivel de Red:

- **Encaminamiento:** Procedimiento por el que un paquete de información puede ser intercambiado entre cualquier par de equipos en una red de comunicaciones.

La arquitectura TCP/IP define un funcionamiento de red de datagramas en su capa de red:

- Cada paquete de información incorpora dirección origen y dirección destino.
- En cada router se decide cuál es el siguiente salto que ha de realizar cada paquete.

- **Protocolo IP. RFC 791:** Define un sistema de numeración para identificar máquinas en una red y un formato de paquete de nivel de red (interred) para el control del encaminamiento (cabecera IP).

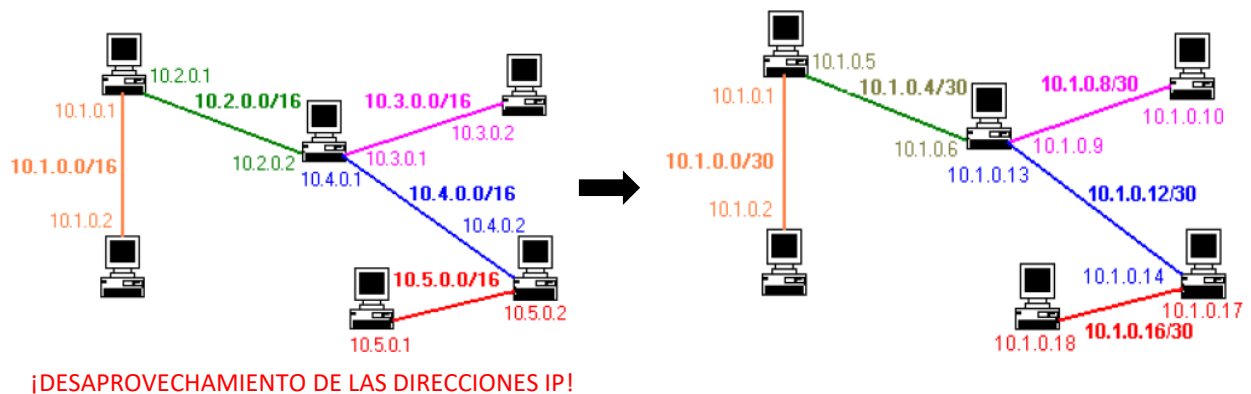
Direccionamiento IP

Clase	7bit	24bit	
A	0	Red	Máquina
			0.0.0.0 127.255.255.255
B	1 0	14bit	16bit
		Red	Máquina
			128.0.0.0 191.255.255.255
C	1 1 0	21bit	8bit
		Red	Máquina
			192.0.0.0 223.255.255.255
D	1 1 1 0	28bit	
		Multicast	
			224.0.0.0 239.255.255.255
E	1 1 1 1 0	27bit	
		Futuras Ampliaciones	
			240.0.0.0 247.255.255.255

Clases de direcciones IP

- **Direccionamiento de redes con el protocolo IP:**

- **Redes de difusión:** Todas las estaciones que comparten un mismo medio físico en una red de difusión tienen que tener asignada la misma dirección de red IP. La elección de la clase se determina dependiendo del número de máquinas en el segmento.
- **Redes Punto a Punto:** Las estaciones en los extremos de una red punto a punto tienen que tener asignada la misma dirección de red IP. Por cada enlace punto a punto se especifica una dirección de red IP. Para evitar la reserva innecesaria de direcciones IP, la máscara de red en una línea punto a punto se escoge para reservar el número de direcciones IP necesarias. Ejemplo: 2 direcciones para máquinas, 1 para red y 1 para difusión.



- **Enlaces multipunto a punto:** Ofrece varias rutas desde una única ubicación a varios lugares.

- **Tablas de encaminamiento:**

- Dispositivos que precisan tablas de encaminamiento:
 - **Estación, PC, host de la red:** Precisa de una tabla de encaminamiento **sencilla**. Una entrada para la red a la que pertenece y otra para la puerta de enlace.
 - **Router** (encaminador de la red): Precisa de una tabla de encaminamiento **compleja**. Necesita entradas en la tabla de encaminamiento para cada red que conoce y una para la puerta de enlace.
- Formato: Una tabla de encaminamiento consta de una fila (entrada) por cada red IP que conoce el router.

Se distinguen 3 tipos de entrada:

- Entradas **asociadas a redes conectadas directamente** (la puerta de enlace es una dirección IP **del** router).
- Entradas **asociadas a redes alcanzables** (la puerta de enlace es la dirección IP de **un** router).
- Entrada **de la puerta de enlace por defecto** (la puerta de enlace es la dirección IP de **un** router).

- **Congestionamiento en redes IP:**

Una red de conmutación de paquetes presenta congestión si al **aumentar** el **flujo** de paquetes de **entrada** a la red (número de paquetes por segundo que entran en la red), **disminuye** el **flujo** de paquetes de **salida** (número de paquetes por segundo que salen de la red).

- Las **causas** son:

- **Routers con insuficiente capacidad de proceso.**

Detección: Es necesario monitorizar cuál es el porcentaje de uso de la **CPU** de los routers. Si el valor de utilización es superior al **60-70%**, se hace necesario emplear un router con mayores prestaciones.

- **Fragmentación de la información con el protocolo IP.** Los routers precisan más tiempo para encaminar la misma información que con un MTU más grande, ya que tienen que analizar más cabeceras IP.

Detección: Es necesario **verificar** que los **MTU** de la red están elegidos adecuadamente y que la fragmentación se evita con mecanismos como la norma RFC 1191.

- **Corrección** del congestionamiento:

Si en una red se detecta una situación de congestionamiento, hay una única solución para que la red no quede bloqueada, **reducir el flujo de entrada** de paquetes a la red. Esta estrategia es empleada por el protocolo **TCP** el cual es capaz de reducir su flujo de transmisión si no llegan los ACKs debido a la congestión.

- **Características** de los **core routers** (routers del **troncal**, con mucha capacidad de procesamiento):

- **Conocimiento de todos los destinos de Internet.** Tablas de encaminamiento grandes y complejas.
 - **Simplificación de las tablas de rutas.** Conocimiento parcial de la red con rutas por defecto. Provocan inconsistencias (destinos inexistentes) y rutas no óptimas.
 - **Gestión de las tablas de encaminamiento.** Manual o automático.

- **Algoritmos de gestión** de tablas de encaminamiento:

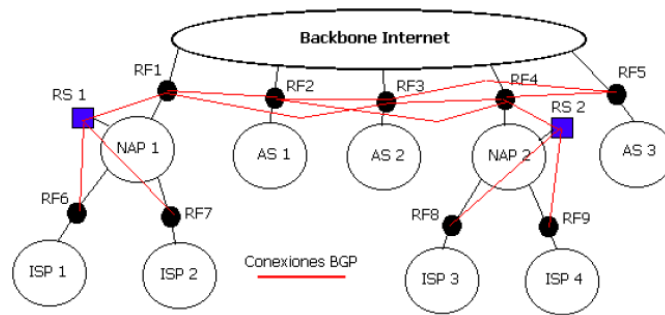
- **Sistema autónomo (SA):** Conjunto de redes y routers controlados por una única autoridad administrativa (un único gestor de políticas de encaminamiento).
 - **Política de encaminamiento:** Conjunto de estrategias o directrices para decidir cuáles son los caminos óptimos a seguir en una red de comunicaciones.

- Protocolo de encaminamiento **BGP** (Border Gateway Protocol): Protocolo para el intercambio de información de encaminamiento entre sistemas autónomos. En cada **SA** se especifica un router de frontera (o más, en general uno) que dialoga con los routers de frontera de otros sistemas autónomos. La información de encaminamiento se intercambia empleando conexiones TCP (puerto servidor 179) entre routers de frontera.

Funcionamiento: Este protocolo se fundamenta en el establecimiento de una conexión TCP para el intercambio de diferentes mensajes BGP. Cada mensaje BGP consta de un paquete con cabecera y datos. La cantidad de datos y su formato depende del tipo de mensaje BGP.



Para conseguir conectividad en Internet todos los sistemas autónomos tienen que estar conectados al backbone de Internet para intercambiar mensajes BGP. En cada NAP (Network Access Point) acceden los sistemas autónomos de varios ISPs (Proveedor de Servicios de Internet) que intercambian información de encaminamiento con BGP entre el backbone de Internet y los ISPs.



Conclusiones:

- **BGP solo informa de accesibilidad, no de rutas a seguir.**
- **BGP establece conexiones entre pares de routers frontera.**
- **BGP informa sobre destinos existentes y no existentes.**

- **Protocolo de Información de Encaminamiento (RIP):**

Se fundamenta en un algoritmo de **vector de distancia (Algoritmo de Bellman-Ford)**. Cada router dispone de una tabla con información de destinos y una métrica (número de saltos) para alcanzar el destino. Cada router propaga la información de sus rutas conocidas a través de mensajes en la red y los routers que la reciben actualizan sus tablas si encuentran rutas más cortas a un mismo destino.

Para cada entrada en la tabla de rutas (distancia, métrica) existe un **temporizador** (180 seg). **Si la ruta no es informada** (distancia, métrica) de nuevo en ese tiempo, **es eliminada**, así evitamos bucles infinitos.

- **Protocolo Abierto del Camino más Corto Primero (OSPF):**

Se fundamenta en el denominado **estado del enlace**, asignando un coste dependiendo de las características del enlace. El conjunto de routers de una red que emplean OSPF conforman un grafo, donde se determinan las rutas más cortas entre cualquier par de nodos empleando el **algoritmo de Dijkstra**.

- **Multicasting:**

Para este propósito está definida la clase D del direccionamiento IP, pudiendo establecer 228 direcciones de multidifusión, o lo que es lo mismo, de grupos de máquinas.

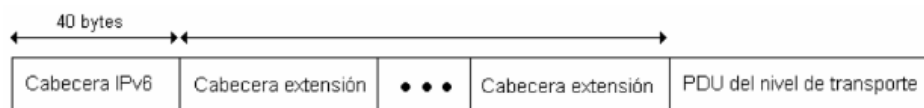
Cada dirección de multidifusión tiene asociada una función específica, de forma que cada dirección de multicast identifica **grupos de máquinas** en Internet que llevan a cabo una función común.

- Cuando un paquete IP se envía a una dirección multicast, si soporta multicasting para cada dirección IP de multicast se asocia una dirección de enlace de multicast. Ejemplo: Ethernet.
- **IGMP (Protocolo de Gestión de Grupo en Internet):** Este protocolo, que al **igual** que **ICMP** funciona sobre IP estableciendo diferentes tipos de mensajes IGMP, permite la gestión del encaminamiento **con multicasting**.

IPv6 (RFC 2460).

- **Limitaciones del IPv4:**

- La principal limitación que ha conducido a la introducción de una nueva versión de protocolo IP es la limitación **en el direccionamiento IPv4 a 32 bits**.



- **IPv6** introduce direcciones IP de **128 bits**, lo que supone disponer de aproximadamente 6×10^{23} direcciones por metro cuadrado de la superficie terrestre. La fragmentación provoca un efecto nocivo en el rendimiento de la red, por lo que **IPv6 no permite la fragmentación** de un paquete IP en un router intermedio.

Formato de la cabecera:

- Clase de tráfico: Permite establecer clases distintas de tráfico.
 - Etiqueta de flujo: Permite identificar flujos de paquetes entre dos aplicaciones origen y destino.
 - **Longitud carga útil**: Tamaño en bytes de las cabeceras de extensión y la PDU de nivel superior.
 - Cabecera siguiente: Especifica qué cabecera sigue a la IPv6. Puede ser una cabecera de extensión o un protocolo de nivel superior (TCP, UDP).
 - **Límite de saltos**: Establece el número máximo de saltos de un paquete IP, al igual que en IPv4.
 - Dirección IP origen y destino: Especifica entre qué interfaces se intercambian los datos.
 - **Anidamiento de cabeceras extendidas en IPv6**: Cuando un dispositivo analiza un paquete IPv6 recorre todas las cabeceras existentes (IPv6 y extendidas) empleando el campo 'cabecera siguiente', hasta que encuentra la cabecera de nivel superior y envía los datos a la capa superior.
- **Direcciones del IPv6**:

Introduce un nuevo sistema de direccionamiento. Una característica fundamental es que son **dinámicas y únicas**. La dirección asignada a un interfaz es de un valor de 128 bits, combinación de la MAC del interfaz y del proveedor de acceso que emplea. Así, el proceso de **encaminamiento es mucho más rápido en los routers**, pues permite establecer **jerarquías de direccionamiento más realistas** como por operador, proximidad geográfica, etc.

3 tipos distintos de direcciones IP:

- Direcciones de unidifusión (**unicast**): Identifican a un interfaz individual.
- Direcciones de multidifusión (**multicast**): Identifica a un conjunto de interfaces que pertenecen a un grupo definido.
- Direcciones de monodifusión (**anycast**): Identifica a un conjunto de interfaces que pertenecen a un grupo, pero el paquete solo se entrega a la interfaz más cercana.

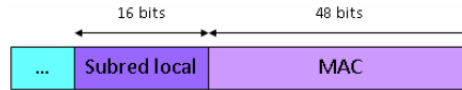
La notación de una dirección IPv6 se establece en 8 grupos de 4 dígitos hexadecimales separados por el símbolo ':' → 2001:BA98:7654:3210:FEDC:BA98:7654:3210

Es posible reducir la notación de una dirección IPv6 omitiendo los grupos que contengan ceros y empleando doble ':' → 2001:BA98:0000:3210:0000:BA98:0000:3210 ↔ 2001:BA98::3210::BA98::3210

❖ Formato de una dirección unicast:



❖ Formato del campo Interface:



El valor de subred local es asignado por el administrador de la red donde se encuentra el dispositivo. Con este esquema, cualquier dispositivo conectado a una red IPv6 tiene un valor dinámico (cambia según la red física en la que se conecte) pero único y reservado para él (debido a la MAC única). Esta característica facilita la movilidad (conocimiento de la ubicación) y titularidad (identificación) de los dispositivos de comunicación IPv6.

• Transición IPv4 – IPv6:

Un dispositivo IPv4 solo puede tener conectividad con dispositivos con IPv4, por tanto, si es necesaria **conectividad IPv4-IPv6** entre dispositivos es necesario disponer de **dos pilas de protocolo IP en paralelo**.

Cuando la conectividad es entre equipos con la **misma versión** de protocolo (IPv4 o IPv6) y deben atravesar una **red intermedia con una versión de IP distinta**, se recurre al procedimiento del **túnel**.

Este procedimiento encapsula un paquete IPv4 (IPv6) como dato dentro de un paquete IPv6 (IPv4) para su transporte en esa red intermedia.

Tema 6:

Nivel de transporte.

➤ **UDP:** El protocolo UDP (Protocolo de datagramas de usuario) está definido en **RFC 768**.

Las características principales:

- Sin conexión.
- Trabaja con paquetes o datagramas enteros, no con bytes individuales como TCP.
- No es fiable. No emplea control del flujo ni ordena los paquetes.
- Provoca poca carga adicional en la red.
- Un paquete UDP puede ser fragmentando por el protocolo IP.
- Admite utilizar como dirección IP de destino la dirección de broadcast.



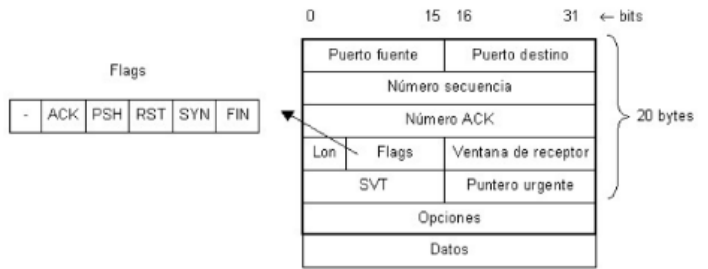
Aplicaciones:

- Transmisión de datos en LANs fiables. Por ejemplo, con TFTP.
- Operaciones de sondeo. Protocolos DNS, SNMP y NTP, servicios echo y daytime.

- **TCP:** El protocolo TCP (Protocolo de control de la transmisión) está definido en **RFC 793**.

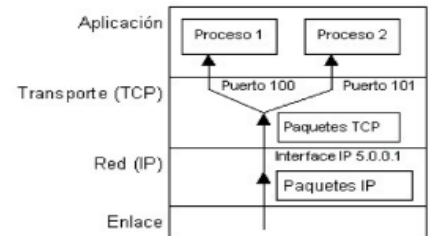
Las características principales:

- Trabaja con un flujo de bytes.
- Transmisión orientada a conexión.
- Fiable. Emplea control de flujo.
- Flujo de bytes ordenado.



- **Multiplexión de conexiones.**

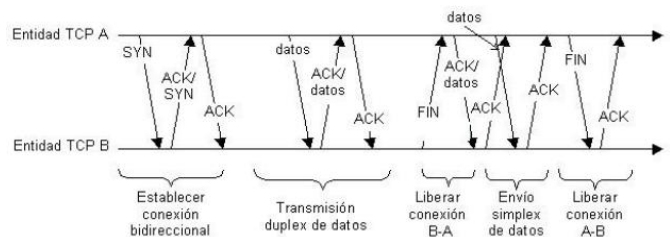
La capa de transporte soporta múltiples conexiones entre un par de equipos empleando el número de puerto para separar los paquetes IP de cada conexión.



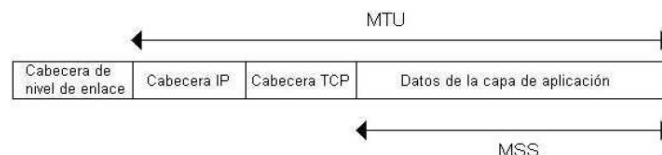
- **Gestión de la conexión.**

- Secuencia de funcionamiento de **TCP**:

- Establecimiento bidireccional de la conexión.
- Intercambio de datos.
- Liberación bidireccional de la conexión.



- **MSS** (Maximum Segment Size): Cantidad máxima de datos que puede incorporar un paquete (segmento) TCP. Este valor **depende del MTU** de la red donde se transmite el paquete TCP. Para **evitar la fragmentación IP**, en el establecimiento de la conexión se negocia el valor del MSS. Este valor **se intercambia en el campo de opciones de los paquetes SYN**.



- **Control de flujo de datos.**

- Si la red no proporciona ningún mecanismo para controlar la congestión, este ha de llevarse a cabo con los protocolos de la arquitectura de red. El protocolo de la capa de transporte TCP es un protocolo que presenta las siguientes características:
 - Protocolo fiable con confirmación de paquetes.
 - Transmisión orientada a conexión.
 - Control del flujo de bytes.
- El control del flujo se realiza **variando el tamaño de la ventana del receptor** (campo window en la cabecera TCP):
 - Si la **ventana del receptor aumenta**, el emisor puede enviar más información sin esperar a recibir ACK (**aumenta** ventana del **emisor**).
 - Si la **ventana del receptor disminuye**, el emisor envía menos información sin esperar a recibir ACK (**disminuye** ventana del **emisor**). Caso límite: Window = 0.

- **Pérdida de segmentos. Reenvío de la información.**

Si un segmento no llega al receptor o llega con errores, el receptor no enviará ACK. Los siguientes segmentos que envíe el emisor (hasta su tamaño de ventana máximo) se almacenarán en el buffer del receptor, pero este enviará ACK de la secuencia previa al paquete erróneo.

- **Cálculo del tiempo de espera de ACK. Algoritmo de Karn.**

El tiempo de espera de un ACK (**Timeout**) debe ser calculado de forma que sea lo suficientemente:

- **Grande** para evitar que los retardos en la red no provoquen reenvíos innecesarios por retardos en el envío del ACK.
- **Pequeño** para que no haya periodos de inactividad en el envío de datos en la red.

- **Control de la congestión en TCP. RFC 2581.**

La congestión en una red es una situación de **retardo elevado** en el envío de información, debido a la **sobrecarga de encaminamiento** en los routers de una red. Para reducir la congestión, TCP debe reducir la tasa de envío de datos, es decir, **reducir su ventana del emisor**.

- **Prevención de la congestión por decremento multiplicativo.**

Esta técnica se fundamenta en la definición en el emisor de una nueva ventana denominada **ventana de congestión**, un valor en bytes al igual que la ventana del emisor.

En todo momento, la ventana del emisor se calcula como el valor mínimo de dos valores: la ventana de congestión y la ventana que informa el receptor.

- **Recuperación de una situación de congestión. Algoritmo de inicio lento.**

Una vez que se evita la congestión y comienzan a llegar ACKs, el timeout vuelve a decrementarse y la ventana de congestión debería aumentar. La recuperación se realiza más lentamente. Para ello, *el valor de la ventana de congestión se incrementa en un tamaño de MSS bytes, cada vez que el emisor recibe un ACK.*

- **Problema de los paquetes pequeños. Algoritmo de Nagle. RFC 896.**

Si una aplicación envía a la capa TCP información en bloques de pocos bytes, puede producirse una situación de desaprovechamiento del medio físico. El emisor enviará bloques de un byte al receptor y este hará ACKs de un byte.

*Para evitar que el intercambio de datos sea byte a byte, el algoritmo de Nagle hace que TCP agrupe los bytes enviados por la aplicación en un segmento TCP. El primer byte será enviado y TCP almacena los bytes que lleguen del nivel superior hasta la llegada del ACK. A continuación, enviará todos los bytes acumulados en otro segmento, y acumulará los siguientes hasta la llegada del ACK. Si se alcanza el tamaño del MSS en el **buffer**, TCP envía el segmento sin esperar al ACK.*