

Servicios que ofrece el nivel de red:

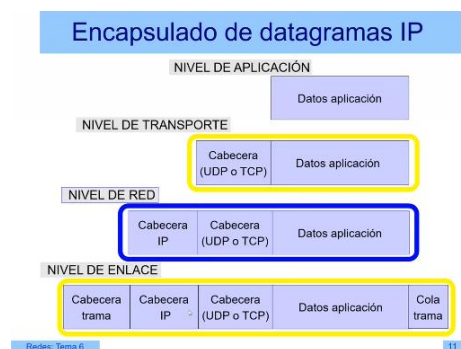
- Servicios a nivel de paquete individual:
  - Entrega garantizada
  - Entrega garantizada con retardo limitado
- Servicios para un flujo de paquetes:
  - Entrega en orden
  - Ancho de banda mínimo garantizado
  - Fluctuación máxima garantizada
  - Servicios de seguridad
    - Confidencialidad, integridad, autenticación, etc.

Redes de conexión o sin conexión:

- Con conexión: establecer conexión a nivel lógico, los routers intermedios intervienen en el proceso.
- Sin conexión: Redes de datagramas (para cada paquete se plantea por donde se envía).
- Con conexión en nivel transporte vs. Nivel de red:
  - Transporte: entre dos procesos
  - Red: entre dos hosts (routers están involucrados)

Redes de datagramas: El paquete solo se envía, el destino va en la cabecera. Los paquetes se envían en los routers usando la dirección destino, todos los paquetes son independientes, y no sabemos si llega o no.

El router puede recibir datos de una trama y reenviarlos a otra trama.



Para poder llevar los paquetes a través de la red se necesita:

- Identificar los sistemas que interviene (direcciones IP).
- Elegir una ruta para alcanzar el destino (encaminamiento).

Forwarding (reenvío): el router mueve los paquetes que recibe de un enlace de entrada a uno de salida (tablas de reenvío).

Routing (encaminamiento): calcular la ruta a tomar por los paquetes de origen a destino (algoritmos de enrutamiento).

## 2) IP v4. (Internet Protocol):

Funciones del nivel de red:

- Protocolos de enrutado:
  - Selección de una ruta
  - RIP, OSPF, BGP
- Protocolo IP:
  - Normas de direccionamiento

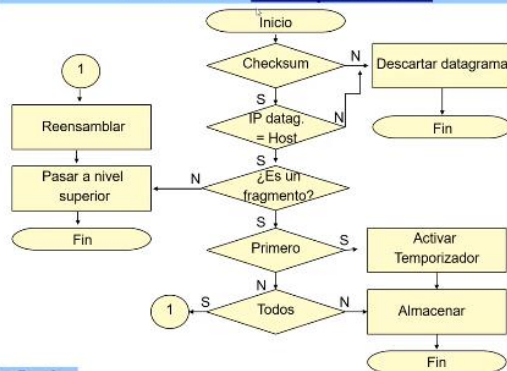
- Formato del datagrama
- Reglas de manejo de datagramas
- Protocolo ICMP:
  - Informe de errores
  - Mensajes de control

IP v4 es el protocolo central de la pila de protocolos TCP/IP, y es sin conexión, no mantiene información de estado sobre los datagramas y cada datagrama se maneja de forma independiente.

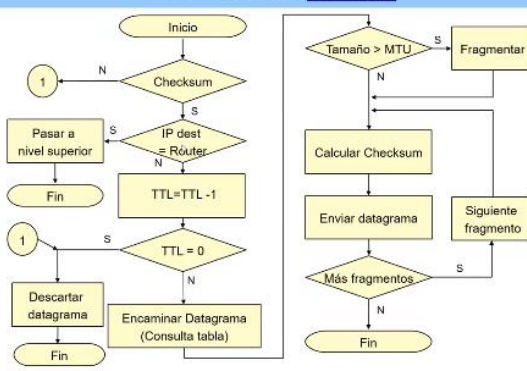


- Versión Protocolo: 4 bits
- Longitud cabecera: 4 bits
- Longitud total del datagrama: cabecera y datos. Tamaño máximo = 65535 bytes.
- Tipo de servicio: 3 bits prioridad, 4 bits tipo servicio (usuario pone un bit a '1') y un bit a cero.
- Identificación, Flags y Desp. Fragmento -> FRAGMENTACIÓN, que es regulada por la MTU (máximo tamaño transferencia).
- Tiempo de vida (TTL): se suele inicializar a 64 en el origen, cada vez que pasa por un router se decrementa, cuando llega a 0 se descarta.
- Protocolo: indica el protocolo al que corresponden los datos (TCP 6, ICMP 1 y UDP 17).
- Checksum: exclusivo de la cabecera.
- Opciones: especifica encaminamiento fuente, confidencialidad del datagrama, registrar la ruta. Es de longitud variable.

### Procesamiento de un datagrama IP en un computador



### Procesamiento de un datagrama IP en un router



**2) IP v4. (Internet Protocol) continuación:**

- Una máquina puede tener varias direcciones IP.
- Son direcciones virtuales y tienen tamaño fijo de 32 bits.
- Van por octetos (n1.n2.n3.n4). Ejemplo:
  - 10000000 00001010 00000010 00011110
  - 128.10.2.30
- Las direcciones IP tienen dos campos: Identificador de red e Identificador computador en la red. Todos los hosts y routers en la misma red poseen el mismo identificador de red.

Todos los dispositivos conectados a la red necesitan una dirección IP, y los routers tienen al menos dos (lo que hay a cada lado de un router es una red IP).

**Direcciones IP especiales:**

- Dirección IP de una red: Id.red + "0"
  - Se refiere a la red y no a sus computadores
- Dirección Loopback: 127 + cualquier cosa
  - No envía paquetes por la red
- Dirección de este host: Todo a "0"
  - Dirección fuente cuando el host obtiene su IP automáticamente
- Dirección difusión dirigida: Red + todo a "1"
  - Se entrega a todos
- Dirección difusión limitada: Todo a "1"
  - Entrega en la red IP donde está conectado el host.
  - Dirección destino durante el arranque del sistema si el host aun no conoce su dirección de red

**Direcciones privadas:**

- No encaminables por los routers de Internet
- 3 rangos de direcciones privadas
  - ID Red de 8 bits: 10
    - Rango: 10.0.0.0 – 10.255.255.255
  - ID Red de 12 bits: 172.16
    - Rango: 172.16.0.0 – 172.31.255.255
  - ID Red de 16 bits: 192.168
    - Rango: 192.168.0.0 – 192.168.255.255

**Tipos de direccionamiento:**

- Direccionamiento con clases (obsoleto)
- Direccionamiento sin clases (máscara)

**Direccionamiento sin clases:**

- Bits fijos (prefijo de red)
- Bits variables (bits de host)
- Prolonga la vida de IPv4, IPv6 utiliza esta visión sin clases y gracias a esto, nace la fragmentación.

- Máscara de red: saber cuántos bits son del prefijo de red y cuantos son de host.  
Ejemplo para 20 bits a "1":
  - 255.255.240.0 -> de aquí los 255 ( $2^8$ ) por lo que serían 16 bits + el 240 ( $2^4$  del campo de 8 bits) todos a "1", por lo que son 20 bits para el prefijo de red.
  - Es lo mismo que decir Dir IP/20

## Direcciones IP fuente y destino

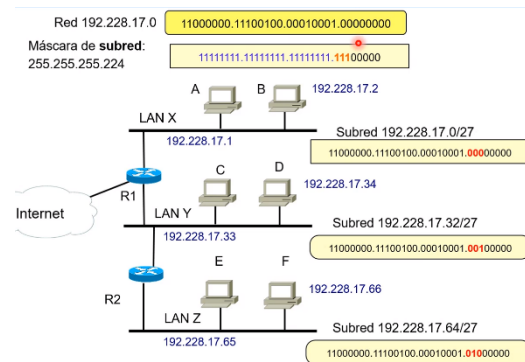
- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>• IP fuente:           <ul style="list-style-type: none"> <li>– No es dirección de red</li> <li>– No es dirección de difusión</li> <li>– No está en rango reservado               <ul style="list-style-type: none"> <li>• (<math>\geq 240</math>. XX.XX.XX o 1111...)</li> </ul> </li> <li>– <i>Loopback</i>: condiciones restringidas</li> <li>– Todos los octetos <math>\leq 255</math></li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• IP destino:           <ul style="list-style-type: none"> <li>– No es dirección de red</li> <li>– No es dirección 0.0.0.0</li> <li>– No está en rango reservado               <ul style="list-style-type: none"> <li>• (<math>\geq 240</math>. XX.XX.XX o 1111...)</li> </ul> </li> <li>– <i>Loopback</i>: condiciones restringidas</li> <li>– Todos los octetos <math>\leq 255</math></li> </ul> </li> </ul> |
|--|---|

### Tablas de reenvío:

- Deben ser pequeñas y compactas.
- Contienen: Dirección IP red destino, mascara de red, dirección IP siguiente router, interfaz de salida.

### Subredes:

- Tenemos una dirección de red 192.228.17.0/24
  - 192.228.17.0 = 11000000 . 11100100 . 00010001 . 00000000
  - Máscara inicial: 255.255.255.0 = 11111111 . 11111111 . 11111111 . 00000000
  - Una red, 254 direcciones ( $2^8$ , pero no se puede usar la combinación todo "0" ni todo a "1" porque es la dir. Difusión).
- La dividimos en subredes:
  - Pasamos bits del campo de host al campo de red (bits de la última parte de la derecha a formar parte de la izquierda, en este caso del ultimo byte).
  - Nueva máscara de red: /27
  - 255.255.255.224 = 11111111 . 11111111 . 11100000
  - 3 bits de subred equivalen a 8 redes ( $2^3$ ).
  - 5 bits de host (los últimos) equivalen a 30 hosts ( $2^5 - 2 = 32 - 2 = 30$ ).



### Superredes:

Ejemplo: Las 8 redes desde 194.32.136.0 a 194.32.143.0 tienen un prefijo común de 21 bits:

- 194.32.136.0/24 = 1100000010 00100000 10001000 00000000
- 194.32.137.0/24 = 1100000010 00100000 10001001 00000000
- ...
- 194.32.143.0/24 = 1100000010 00100000 10001111 00000000

Se pueden agrupar como: 194.32.136.0/21

## Tema 6. El nivel de Red A4

03/03/2021

### Obtención de una dirección de red:

- Configurada manualmente por el administrador del sistema.
- Mediante el protocolo de configuración de host DHCP.
- El ISP consigue un bloque de direcciones a través del ICANN (ya no hay bloques libres para repartir).

### IPv6:

- Se crea para prevenir tener redes a futuro.
- Soporte de audio y video.
- Cabeceras mas flexibles que en IPv4 para agilizar el encaminamiento.
- Direcciones de 128 bits.
- Tipos de direcciones:

- Unicast: dirección de un computador.
- Multicast: dirección de un grupo de computadores (todos).
- Anycast: dirección de un grupo de computadores (uno de los computadores del grupo, el más cercano).

Tipo Dirección	Prefijo (bin)	Prefijo (Hex)
Reservada	0000 0000	0000:: /8
Unicast global	001	2000:: /3
Unicast organización local	1111 1110 10	FE80:: /10
Unicast sitio local (en desuso)	1111 1110 11	FEC0:: /10
Unicast local (ULA)	1111 110	FC00:: /7
Multicast	1111 1111	FF00:: /10

- Notación hexadecimal.

### Algoritmos de enrutamiento:

- Los algoritmos de enrutamiento son representados mediante un grafo:
  - Vértices -> routers
  - Aristas -> enlaces entre routers
- Los grafos son no dirigidos (el camino es de ida como de vuelta).

### Criterios de clasificación:

- ¿Escalable? Algoritmos por vector de distancias y estado del enlace como máximo para 100 routers.
- ¿Centralizado o distribuido? Depende de donde se calculen las tablas. Los centralizados son difíciles de escalar.
- Según la frecuencia:
  - Estáticos: suelen actualizarse manualmente.
  - Dinámicos: son sensibles a cambios en el tráfico o en la topología de la red.

### Enrutamiento por estado del enlace:

- Cada router debe:
  - Descubrir sus vecinos y conocer sus direcciones de red.
  - Medir el coste a cada vecino.
  - Crear un paquete con la información.
  - Enviar el paquete a TODOS los routers de la red.
- Con esos mensajes, cada nodo (router):
  - Construye el grafo de la red.
  - Calcula el camino más corto a cada destino.
  - Construye la nueva tabla de reenvío.
- El paquete de estado del enlace contiene:
  - Identidad del emisor.
  - Numero de secuencia.
  - Lista de vecinos y su distancia a ellos.
  - Tiempo de vida (TTL).

### Notación para Algoritmo de Dijkstra:

- $c(i,j)$ : coste del enlace del nodo  $i$  al  $j$ .
- $D(v)$ : valor actual del coste mínimo del camino desde la fuente al destino  $v$ .
- $p(v)$ : nodo predecesor a lo largo del camino desde la fuente a  $v$ , o sea un nodo vecino de  $v$ .
- $N'$ : conjunto de nodos cuyo camino de mínimo se conoce definitivamente.

#### Ejecución del algoritmo de Dijkstra

Para el nodo fuente A

Paso	N'	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	4, A	infinito	infinito	5, A	infinito
1	A, B		6, B	infinito	5, A	10, B
2	A, B, E		6, B	infinito		10, B
3	A, B, E, C			9, C		10, B
4	A, B, E, C, D					10, B
5	A, B, E, C, D, F					

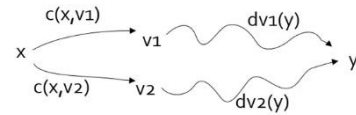
#### Tabla de reenvío de A

Destino	Enlace
B	(A,B)
C	(A,B) / (A,E)
D	(A,B)
E	(A,E)
F	(A,B)

Paso	N'	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	4, A	infinito	infinito	5, A	infinito
1	A, B		6, B	infinito	5, A	10, B
2	A, B, E		6, B	infinito		10, B
3	A, B, E, C			9, C		10, B
4	A, B, E, C, D					10, B
5	A, B, E, C, D, F					

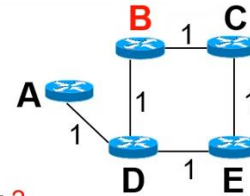
Enrutamiento por vector de distancias:

- Cálculo de la distancia a un destino:
  - Coste de la ruta mínima de X a Y (ecuación de Bellman-Ford):  $D_x(y) = \min_v \{c(x,v) + d_v(y)\}$
- Con las distancias desde cada vecino se construye la tabla de distancias
- Y a partir de la tabla de distancias la de reenvío.



• Información disponible en el nodo B:

- Vecinos: C y D
- Distancia a los vecinos:  $d_B(C) = 1$ ,  $d_B(D) = 1$



• Distancia del nodo B al nodo destino A

$$d_B(A) = \min \{c(B,C) + d_C(A), c(B,D) + d_D(A)\} = \min \{1 + 3, 1 + 1\} = 2$$

Vectores de distancias de los nodos C y D

C		D	
A	3	A	1
B	1	B	1
D	2	C	2
E	1	E	1

$$d_B(C) = 1 \quad d_B(D) = 1$$

Tabla de distancias del nodo B

Destino	Coste al destino vía	
	C	D
A	4	2
C	1	3
D	3	1
E	2	2

Tabla de reenvío

Destino	Siguiente salto
A	D
C	C
D	D
E	C

- $D_x(y)$  = coste mínimo estimado desde X hasta Y
  - El nodo X mantiene el vector de distancias  $D_x = [D_x(y); y \in N]$
- Nodo x:
  - Conoce el coste a cada vecino V:  $c(x,v)$
  - Mantiene los vectores de distancia de sus vecinos. Para cada vecino V, X almacena:  $D_v = [D_v(y); y \in N]$
  - Si no conoce la distancia a un destino  $D_x(y) = \infty$

La idea básica es que cada uno nodo envía periódicamente su vector de distancias y siempre que X recibe el vector de distancias de un vecino, X actualiza su propio vector de distancias mediante la ecuación  $D_x(y) \leftarrow \min_v \{c(x,v) + D_v(y)\}$  para cada nodo  $Y \in N$

Cambios en el coste de un enlace:

- Los cambios en los costes a veces se resuelven rápidamente

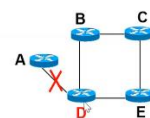
Destino	Coste al destino vía:	
	C	D
A	4	2
B	2	2
C	1	3
D	3	1

• Solución con inversa envenenada

Destino	Coste al destino vía		
	A	B	E
A	$\infty$	$\infty$	$\infty$
B	$\infty$	1	3
C	$\infty$	2	2
E	$\infty$	3	1

Pero C ofrecerá a B una ruta a A a través de E

Más iteraciones hasta que C detecte que ni B ni E tienen ruta a A





**Enrutamiento por internet:**

Todos los algoritmos de enrutamiento que vimos antes son “factibles” cuando hablamos de pocos nodos, pero cuando ya hablamos de millones tenemos problemas de convergencia, tráfico, y tablas inmensas de encaminamiento.

Su solución, Sistemas autónomos (AS).

Enrutamiento intra-AS:	Enrutamiento inter-AS:
<ul style="list-style-type: none"> <li>Entre routers en el mismo AS.</li> <li>Todos los routers de un AS deben ejecutar el mismo protocolo de enrutamiento intra-AS.</li> <li>Los routers en diferentes AS pueden utilizar distintos protocolos intra-AS.</li> <li>Routers pasarela (Gateway router): en la “frontera” del AS, se comunican con otros routers AS.</li> </ul>	<ul style="list-style-type: none"> <li>Entre distintos AS.</li> <li>Utiliza los routers pasarela (que además también emplean el protocolo intra-AS).</li> </ul>

Las tablas de reenvío son creadas con ambos tipos de enrutamiento, Inter-AS para destinos externos y el Intra-AS para los destinos del AS.

**Protocolos intra-AS:**

Más comunes:

- Vector de distancias:
  - RIP: Routing Information Protocol
  - IGRP: Interior Gateway Routing Protocol
- Estado del enlace:
  - OSPF: Open Shortest Path First

**OSPF: Open Shortest Path First**

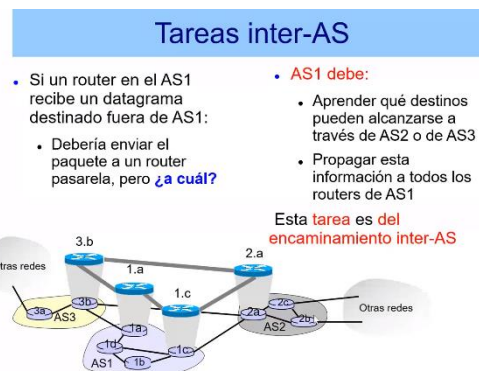
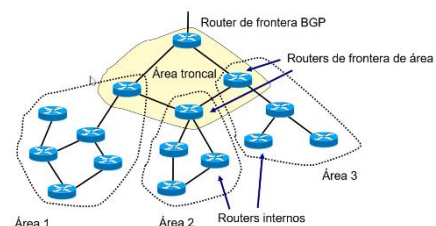
Algoritmo de estado del enlace:

- Difusión de paquetes de estado del enlace a todos los routers del dominio.
- Una entrada en el paquete por router vecino.
- Calculo de rutas mediante el algoritmo de Dijkstra

La información se envía sobre IP.

Características:

- Seguridad: autenticación de mensaje de encaminamiento.
- Permite múltiples caminos con el mismo coste.
- Utilizar diferentes simétricas para el mismo enlace para diferentes tipos de servicio.
- Soporte multicast (especificar grupos de máquinas, y cada máquina perteneciente a un grupo, recibe una copia de cada paquete IP que tu envíes).
- En AS grandes se puede usar OSPF jerárquico.

**OSPF jerárquico**



## Enrutamiento entre AS en Internet: BGP (Border Gateway Protocol)

Permite a cada AS:

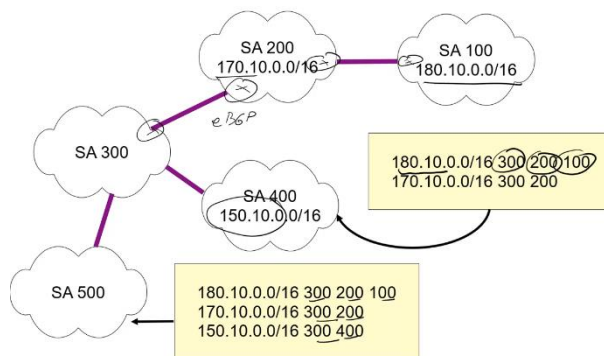
- Obtener información sobre redes destino que se pueden alcanzar a través de otros AS.
- Propagar esa información a todos los routers internos del AS.
- Obtener “buenas rutas” a las redes destino basadas en información de rutas y políticas de los AS.

Además, permite a una red informar de su existencia al resto de Internet.

Funcionamiento de BGP:

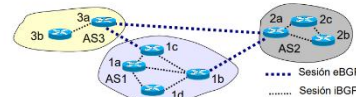
Es un algoritmo por vector de caminos:

- Similar al protocolo por vector de distancias, pero trabaja con rutas completas.
- Cada AS tiene un número de identificación único.
- Cada pasarela informa de la secuencia de AS que se atraviesan hasta alcanzar una red destino.
- Trabajar con rutas completas tiene sus ventajas (impide bucles de encaminamiento).



### Distribución de información

- Con una sesión eBGP entre 3a y 1c, AS3 envía información de alcanzabilidad de prefijo (ej., 138.16.67/24) a AS1.
- 1c puede usar iBGP para distribuir este nuevo alcance de prefijo a todos los routers en AS1.
- 1b puede entonces re-anunciar la información de alcance a AS2 a través de la sesión eBGP entre 1b y 2a.
- Cuando un router aprende del nuevo prefijo, crea una entrada para ese prefijo en su tabla de re-envío.



## Introducción y servicios de nivel:

### Clasificación de redes:

- WAN (Wide Area Network): para continentes.
- MAN (Metropolitan Area Network): entre edificios, por ejemplo.
- LAN (Local Area Network): computadoras conectadas a un router.
- PAN (Personal Area Network): computadora y teléfono propio.

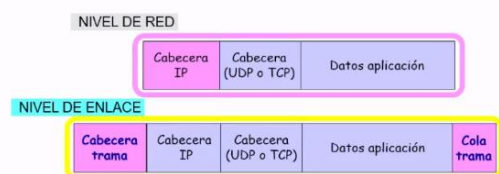
### Características de LAN:

- Cubren un área geográfica moderada.
- Altas velocidades y tasa de error baja.

Capa de Red	Capa de Enlace
De extremo a extremo	De nodo a nodo
Mueve los segmentos de la capa de transporte del sistema origen hasta el destino	Permite que los routers sepan el destino final para saber a quien transmitir el paquete para que llegue a su destino

### Capa de enlace:

- Capa lógica por debajo del nivel de red y por encima del nivel físico.
- Intenta conseguir una comunicación eficiente entre dos nodos directamente conectados.
- Unidad de transferencia: trama.



Los datagramas IP se encapsulan en tramas.

¿Qué ofrece?

- Delimitación de la trama (el formato de la trama depende del protocolo de enlace utilizado).
- Control de flujo (ajustar velocidades entre transmisor y receptor).
- Gestión del canal (define las reglas para poder transmitir una trama en el enlace, así como la comunicación simplex, half-duplex y full-duplex).
  - Simplex: una sola dirección de envío.
  - Half-duplex: se puede enviar o recibir, pero no al mismo tiempo.
  - Full-duplex: se puede enviar mientras se recibe, son 2 cables.
- Detección de errores.
- Entrega segura.

## Detección y corrección de errores:

### Códigos detectores de error:

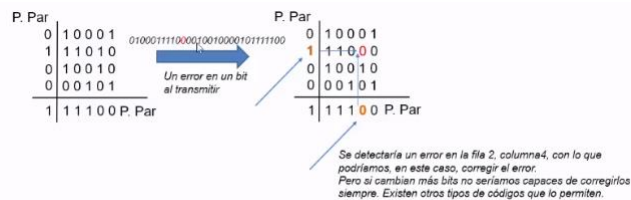
- Paridad.
- Suma de comprobación de internet (checksum).
- Comprobaciones de redundancia cíclica.

**Paridad:**

Añade a cada código de n-bits, 1 bit de paridad para conseguir un numero par/impar de unos en cada byte.

El bit de paridad puede ser 1 o 0 para que:

- Con paridad par: 01001011
- Con paridad impar: 01001010

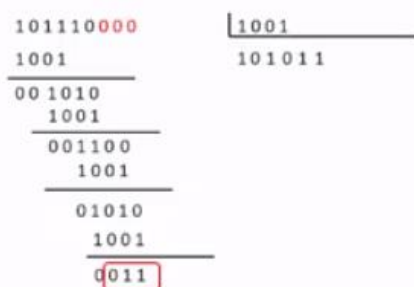
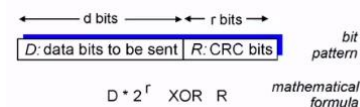


**Suma de comprobación (Checksum)  
de Internet:**

Emisor	Receptor
Los bytes de datos se suman como enteros de 16 bits.	Vuelve a realizar la suma de los datos
El complemento a 1 de la suma es la suma de comprobación a transmitir.	Comprueba si el resultado obtenido es el mismo que el recibido: NO -> error detectado SI -> no se detecta error.

**Códigos de redundancia cíclica: CRC**

- Se tratan los bits de datos, D, como números binarios.
- Se elige un patrón generador de r+1 bits, G.
- Elegir r bits de CRC, R, tal que:
  - $\langle D, R \rangle$  sea exactamente divisible por G.
  - El receptor conoce G, divide  $\langle D, R \rangle$  por G. Si el resto no es cero, se detecta el error.



La información que se transmitirá: 101110011

**Otra forma de calcular el CRC**

$101110 \Rightarrow x^5 + x^3 + x^2 + x^1$   
Lo desplazamos 3 posiciones (añadimos 3 ceros),  
ya que es el grado del polinomio generador (1001),  $G(x) = x^3 + 1$

$x^8 + x^6 + x^5 + x^4$  y dividimos:

$$\begin{array}{r}
 x^8 + x^6 + x^5 + x^4 \\
 \underline{x^8 + x^6 + x^5 + x^4} \\
 x^4 + x^3 \\
 \underline{x^4 + x^3} \\
 x \\
 \underline{x} \\
 1
 \end{array}$$

011. El CRC a añadir cuando se transmite la  
mensaje

- Con un generador de grado r (r+1 bits) se pueden detectar:
  - Todas las ráfagas de error de longitud  $\leq r$ .
  - Todos los errores que afectan a un número impar de bits.

**Corrección de errores:**

- FEC (Forward Error Correction):

- Añade información que permitirá al receptor reconstruir la información correcta.
  - Detección + recuperación.
- ARQ (Automatic Repeat Request):
  - El emisor tiene que retransmitir la información dañada.
  - Detección + reenvío.

**Acceso al medio:****Enlaces y protocolos de acceso múltiple:**

Dos tipos de enlaces:

- Punto a punto
  - Teléfono cableado.
  - Red Ethernet.
- De difusión (cable o medio compartido)
  - Ethernet y LAN inalámbrica.

**Enlaces punto a punto:**

Dedicado entre cada dos nodos, único emisor y receptor.

- Ventaja: canales no compartidos, seguridad y privacidad.
- Inconveniente: cuando crece el numero de nodos (n) se requieren muchos canales.  
 $\text{Conexiones} = n(n-1) / 2$

**Enlace de difusión:**

- Solo un nodo debe usar el canal para transmitir con éxito.
- Si dos o mas nodos transmiten al mismo tiempo -> interferencias y colisión (todas las tramas implicadas se pierden).
- Protocolo de control de acceso al medio -> regula como los nodos comparten en el canal.

**Características de un protocolo de acceso múltiple ideal:**

- Equitativo: el ancho de banda se divide entre los nodos que lo necesiten.
- Descentralizado: no hay nodo maestro que pueda ser el punto de fallo de la red.
- No requiere un reloj global.
- Simple, que no sea costoso implementar.

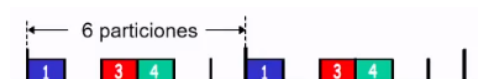
**Taxonomía de los protocolos MAC (Media Access Control):**

Tres grandes clases:

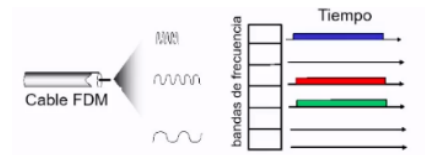
- Partición estática del canal: Canal en pequeños trozos, cada trozo se asigna a un nodo.
- Acceso aleatorio: Canal no preasignado, puede haber colisiones y hay que recuperarse.
- Acceso por turnos: acceso al canal coordinado por turnos para evitar colisiones.

**Partición de partición del canal:**

- Multiplexación por división del tiempo:
  - Se divide el uso del canal en marcos temporales.
  - Partición fija a cada nodo, las que no se usan se pierden.



- Multiplexación por división de frecuencia:
  - Ancho de banda dividido en bandas de frecuencias.
  - Cada nodo tiene su banda de frecuencia.
  - Las bandas que no se usan se pierden.



#### Protocolo de acceso aleatorio:

- El nodo utiliza todo el ancho de banda.
- Si dos nodos transmiten a la vez, hay colisión.
- Especifica: como detectar colisiones y como recuperarse de una colisión.
- Solución: CSMA, escucha la señal portadora antes de transmitir. Canal libre transmite, canal ocupado retrasa la transmisión.

#### Protocolos de acceso por turnos:

- Hacer un anillo lógico para saber quien va antes y quien después.
- Cuando se recibe el testigo puede transmitir, al acaba el tiempo se pasa el testigo.
- Si un nodo falla, toda la red puede fallar.

Protocolos de partición de carga	Protocolos de acceso aleatorio	Protocolos de acceso por turnos
Eficiente con carga alta Ineficiente con carga baja	Eficiente con carga baja Carga alta -> colisiones	Buscan lo mejor de los otros dos protocolos

### Direccionamiento del nivel de enlace:

#### Direccionamiento del nivel de enlace:

- Direcciones físicas IEEE (8 bytes y los primeros 3 bytes son del fabricante) utilizadas para enviar/transmitir entre interfaces conectados a la misma red física.
- Tipos de direcciones:
  - Unicast: receptor individual.
  - Broadcast: para todos los nodos, todo a "1"s.
  - Multicast: para conjunto de nodos, "1"s en la cabecera de la dirección.

**Direcciones físicas unicast:** cada adaptador de red tiene una MAC unicast.

#### Funcionamiento de ARP:

- Consulta por difusión y luego respuesta privada. Ayuda a conocer la MAC de una máquina.
- El mensaje ARP se envía en el campo de datos de una trama.
- Tipo 0x806 datos ARP, tipo 0x800 datos IP.
- ARP es local a la red (un computador necesita averiguar la dirección física de otro sin compartir la misma red física).

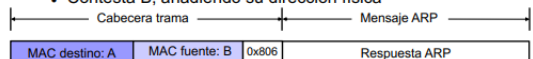
#### • Información en un mensaje de petición ARP

- Dirección física de A, dirección IP de A, dirección IP de B



#### • Información en un mensaje de respuesta ARP

- Contesta B, añadiendo su dirección física

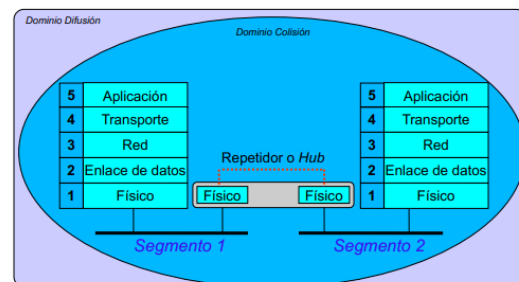


**Dispositivos de interconexión de nivel de enlace:**

- Posibles colisiones: una colisión es cuando dos señales transmiten al mismo tiempo y chocan, y la respuesta final es una fusión de ambas.
- Dominio de colisión: conjunto de estaciones que se ven afectadas por una colisión (tanto si participa en ella como si no)
- Dominio de difusión: conjunto de estaciones que recibe una difusión efectuada por alguna de ellas.

**Repetidores/Hubs:**

- Repetidor: dispositivo electrónico que regenera la señal.
  - No entiende el formato de la trama, ni las direcciones físicas: copia cualquier señal eléctrica (inclusive colisiones).
- Concentradores (Hubs): son repetidores multipuerto.
- Los repetidores/hubs no separan los dominios de la colisión.

**Esquema: Repetidores****Switch (Conmutador):**

- Almacena la trama que recibe por un puerto y la retransmite selectivamente por otro(s), cuando es necesario (difusión, destino en otro segmento, destino desconocido).
  - Analizan solo las direcciones MAC.
  - Plug & Play, aprenden solos.
- No modifican las direcciones de las tramas.
- Separan los dominios de colisión, pero no separan los dominios de difusión.

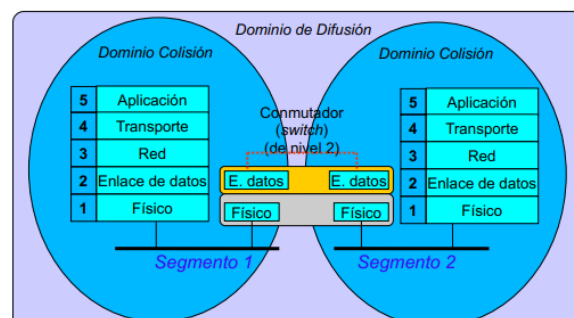
**Conmutadores: auto aprendizaje**

El conmutador aprende que hosts pueden alcanzarse mediante que interfaces (cuando recibe una trama, aprende la dirección origen de la trama y el puerto por el que entró), anota la información en la tabla de retransmisión.

Los conmutadores pueden conectarse de forma jerárquica, conociéndose entre ellos.

**Conmutadores. Limitaciones:**

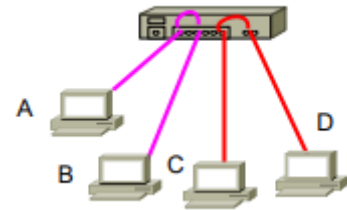
- No separan los dominios de difusión.
- Escalabilidad limitada.
- La cantidad de difusiones aumenta con el número de hosts.
- Las difusiones interrumpen a todos los hosts.
- Un host mal configurado (generando difusiones) entorpece a todo un dominio de difusión.

**Esquema: conmutador**

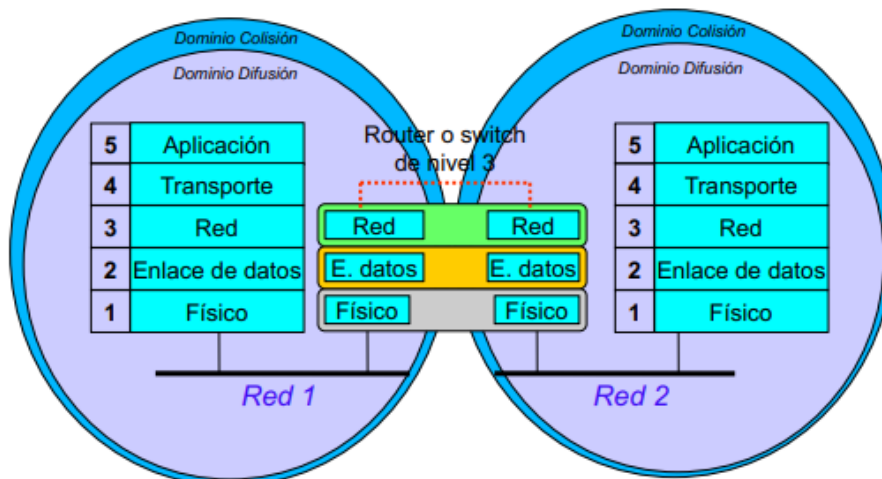


**Switches: transmisiones simultáneas.**

- Permiten transmisiones simultáneas entre varios dispositivos (comunicación full-duplex)
  - Comunicación simultánea entre A-B y C-D sin problemas.
  - Disponen de buffers para almacenar las tramas. No producen colisiones.
  - Mejora de prestaciones respecto a las redes de difusión.
- Pueden conectar segmentos de red con distinto ancho de banda.

**Routers:**

- Permiten la interconexión de redes de igual o distinta tecnología de nivel de enlace. Las decisiones de encaminamiento se toman basándose en las direcciones IP.
- Separan los dominios de difusión y colisión (cada puerto: un dominio de difusión).
- Realizan un procesamiento software de los paquetes recibidos:
  - Decremento TTL, calculo del checksum, fragmentación, generación de paquetes ICMP, algoritmos de encaminamiento.
  - Modifica la dirección origen de la trama original por la suya.
- Tanto los routers como los hosts conectados a ellos necesitan ser configurados con su dirección IP.

**Esquema: Router**

## Ethernet:

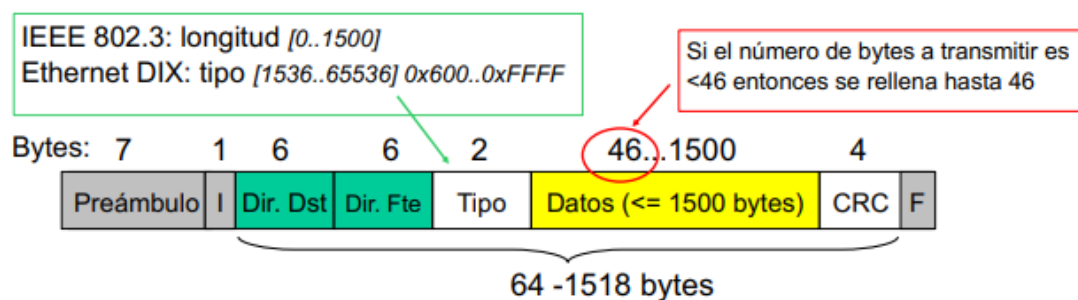
### LAN cableadas: IEEE 802.3-Ethernet

Tecnología LAN cableada “dominante”, barata, fácil de administrar y evolución de velocidad de funcionamiento: 10Mbps – 10Gbps

### Topología en estrella:

- Líneas punto a punto bidireccionales (semi duplex o full duplex).
- El punto central puede ser:
  - Concentrador (hub): estrella de difusión (en desuso).
  - Conmutador (switch): estrella conmutada.

### Formato de trama Ethernet:



- Preámbulo: 7 bytes con el patrón 10101010.
  - Se utiliza para sincronizar emisor y receptor con el reloj del emisor.
- Delimitador de inicio de trama (I): 1 byte con patrón 10101011.
- CRC: no incluye los bits de preámbulo.
- Delimitador de final de trama (F): silencio de 96 bits.

### Ethernet: sin conexión, sin garantías

- No utiliza conexiones.
  - Las tramas se envían directamente y son independientes.
- Sin garantías: no utiliza reconocimientos.
  - Si el contenido de una trama se pierde sólo podrá recuperarse si se utiliza un protocolo de nivel superior con garantías, como TCP
- En topologías de difusión, control de acceso al medio mediante CSMA/CD con *binary exponential backoff*.

### Tecnologías Ethernet:

- Características comunes:
  - Mecanismo de entrega sin garantía.
    - Servicio sin conexión y entrega no fiable.
  - Control de acceso al medio aleatorio (si se requiere): CSMA/CD.

**Ethernet: medios de transmisión**

- Soporte a todas las velocidades sobre diferentes medios de transmisión:
  - Par trenzado.
  - Fibra óptica.
  - Coaxial (al inicio).
- Se definen distancias máximas de los enlaces pendientes del medio de transmisión empleado.

**Configuración mixta. Negocio automático:**

- El negocio automático permite a un par de nodos que comparten un enlace negociar las opciones de funcionamiento.

**Redes inalámbricas:****Elementos de una red inalámbrica:**

- Hosts inalámbricos: pueden ser computadoras, al igual que teléfonos.
- Puntos de acceso:
  - Normalmente conectados a una red cableada.
  - Responsables de reenviar las tramas entre la red inalámbrica y la cableada.

**Diferencias entre redes cableadas y inalámbricas:**

- La potencia de la señal decrece con la distancia mucho más rápidamente.
- Interferencias con otras fuentes de señal.
- Propagación multicamino.

**Problema del terminal oculto:**

- La señal transmitida tiene un alcance limitado
- Dos estaciones no se escuchan porque un obstáculo lo impide o porque la señal no tiene suficiente potencia.

**IEEE 802.11 (LAN inalámbrica):**

- Características comunes:
  - Control de acceso al medio distribuido (CSMA/CA).
  - Mismo formato de trama.
  - Puede reducir su velocidad de transmisión para abarcar distancias mayores.
  - Comparten la misma arquitectura.
  - Compatibles si trabajan en la banda de frecuencias de 2,4GHz.

**Arquitectura de las redes 802.11:**

- La señal transmitida decae con la distancia.
  - El espacio se divide en áreas de alcance de la señal denominadas celdas.
    - Contiene una o más estaciones inalámbricas que pueden ser móviles o fijas.
    - Puede contener un punto de acceso (PA = estación base) que normalmente se conecta a una red cableada.

- Funcionamiento:
  - En una celda pueden coexistir simultáneamente dos modos de funcionamiento:
    - Independiente.
  - Con infraestructura: las estaciones se comunican a través de un punto de acceso.

**Asociación a un PA:**

- Cada PA envía periódicamente una trama de ofrecimiento de asociación (beacon frames):
  - Incluye el SSID y la dirección MAC del PA
- Una estación móvil:
  - Selecciona un PA e intenta la autenticación de la estación:
    - Por dirección MAC.
    - Por nombre de usuario y contraseña para permitir la asociación.
  - Cuando la estación queda asociada a un PA debe obtener una dirección IP de la subred del PA (normalmente mediante DHCP)
  - A nivel de red el PA es transparente (los demás hosts/routers en Internet no ven el PA).

Exploración Pasiva	Exploración Activa
<ol style="list-style-type: none"><li>1. Los PA envían beacon frames.</li><li>2. El host H1 envía una petición de asociación al PA seleccionado.</li><li>3. El PA seleccionado contesta con una respuesta de asociación.</li></ol>	<ol style="list-style-type: none"><li>1. El host H1 envía por difusión una trama de sondeo.</li><li>2. Los PA responden a la trama de sondeo.</li><li>3. El host H1 envía una petición de asociación al PA seleccionado.</li><li>4. El PA seleccionado devuelve una respuesta de petición</li></ol>

**CSMA/CA:**

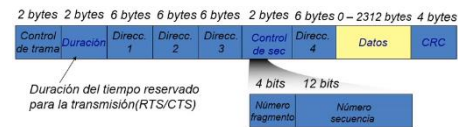
- CSMA/CA emisor:
  - Si detecta el canal libre durante DIFS segundos:
    - Transmite la trama completa (sin escuchar).
  - Si detecta el canal ocupado sigue escuchando:
    - Cuando queda libre espera un tiempo aleatorio (alg. Backoff).
- CSMA/CA receptor:
  - Si trama recibida OK, devuelve ACK después de SIFS segundos (ACK necesario y obligatorio debido al problema de la estación oculta).

**CSMA/CA: Evitación de colisión**

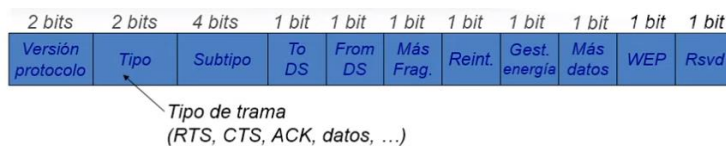
- Una estación solicita al PA transmitir una trama de datos enviado por difusión una trama RTS (request to send).
- El PA contesta enviando por difusión una trama CTS (clear to send):
  - Permite transmitir a la estación solicitante.
  - Prohíbe a las otras estaciones transmitir durante el tiempo indicado.

- Solo se realiza el intercambio de tramas RTS/CTS cuando el tamaño de la trama de datos a enviar supera un umbral definido en la estación.

### Formato de trama 802.11



- Duración / ID de conexión:
  - Campo de duración -> tiempo microsegundos asignado al canal para la transmisión exitosa de una trama MAC.
- Control de secuencia:
  - Subcampo de número de fragmento de 4 bits, usado para fragmentación y reensamblaje, y un numero de secuencia de 12 bits usado para numerar tramas enviadas entre un emisor y receptor dados.
- Datos de la trama:
  - Contiene datos del protocolo del siguiente nivel o información de control MAC.
- CRC: comprobación de redundancia cíclica de 32 bits.



- Control de trama:
  - Indica el tipo de trama y proporciona información de control (incluye si la trama va hacia o desde un DS, información de fragmentación y de privacidad).

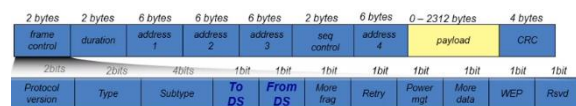
### Tipos de tramas:

- Tramas de control:
  - RTS / CTS / ACK
  - CF-Poll / CF-End
- Tramas de gestión:
  - Beacons
  - Probe Request / Response
  - Association Request / Response
  - Dissociation / Reassociation
  - Authentication / Deauthentication
- Tramas de datos

### ¿Qué es un DS en IEEE 802.11?

Conjunto de servicios que permite conectar un PA a la red cableada o varios PA entre sí

### Trama 802.11: direccionamiento:



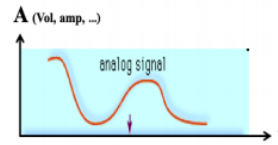
- To DS y from DS:
  - 1 bit cada uno. Si To DS = 1 entonces la trama de datos va destina a un DS y si From DS = 1, la trama de datos fue enviada desde un DS.

- En modo infraestructura:
  - En 802.11 la transmisión de todas las tramas se realizará a través de un PA para llegar a cualquier otro host.
  - PA aparecerá en cada trama de datos 802.11 como transmisor o receptor.
  - Para conservar la dirección MAC de la trama del remitente original o el destino final, se utilizará un tercer campo de dirección.
- Nomenclatura:
  - Dirección destino: MAC del destino final de la trama.
  - Dirección fuente: MAC de la fuente original de la trama.
  - Dirección del receptor: MAC del dispositivo inalámbrico que es el destinatario inmediato de la trama.
  - Dirección del emisor: MAC del dispositivo inalámbrico que está transmitiendo la trama.
- Campos de dirección:
  - Dirección 1, receptor
    - Receptor != PA entonces Receptor = Destino
  - Dirección 2, transmisor
    - Transmisor != PA entonces Transmisor = Fuente
  - Dirección 3, fuente o destino

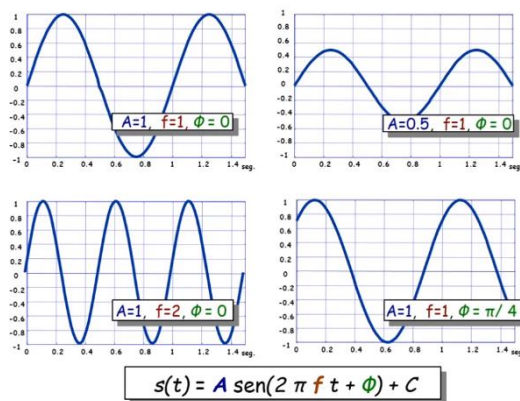


Señales para la transmisión de datos:

- Señal: función que refleje el cambio de una magnitud en el tiempo.
- Tipos:
  - Analógicas vs Discretas (digitales)
  - Periódicas:  $s(t + T) = s(t)$ , periodo  $T = 1/f$
- Señal Analógica:
  - Representa una magnitud de manera continua
  - Decimos que la señal varía de forma “análoga” a la magnitud que medimos
- Señal Digital:
  - Toma valores para una cantidad discreta de puntos
  - Normalmente analógica digitalizada -> cuantificada (limitada en precisión) que se expresa con un número infinito de dígitos -> digital
- Señal Periódica:
  - Patrón de repetición en el tiempo (ciclo)
    - $s(t + T) = s(t)$
  - Periodo (T) = el tiempo de un ciclo (segundos)
  - Frecuencia (f) = factor de repetición (cilos/segundos o Hz)
    - $f = 1/T$
- Señal Aperiódica:
  - No existe un patrón de repetición
  - Periodo (T) = infinito
  - Frecuencia (f) = 0

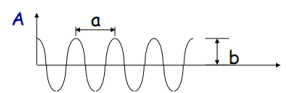


## Señales sinusoidales

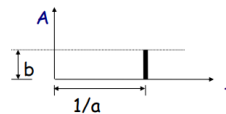


## Representación de las señales

a) Dominio del tiempo



b) Dominio de la frecuencia

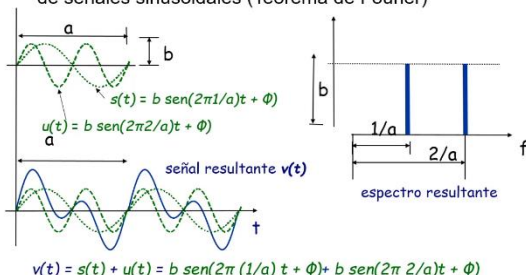


## Espectro de una señal

- Conjunto de frecuencias que constituyen la señal
- Si todas las frecuencias son múltiplos de una dada: cada componente de frecuencia recibe el nombre de armónico

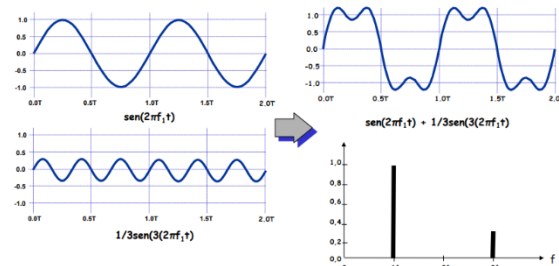
## Representación de las señales

- Las señales periódicas se pueden representar como suma de señales sinusoidales (Teorema de Fourier)



## Representación de las señales

- Una señal digital periódica se puede crear mediante la suma de infinitas señales senoidales





**Componente continua:**

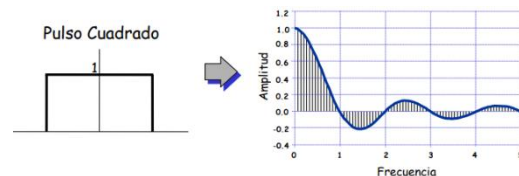
- La componente continua representa el nivel medio de la señal sobre el 0

$$s(t) = A \operatorname{sen}(2 \pi f t + \Phi) + C$$

- No varía en el tiempo -> frecuencia cero
- Causa problemas en los sistemas de transmisión
  - Disipación de energía

**Ancho de banda:**

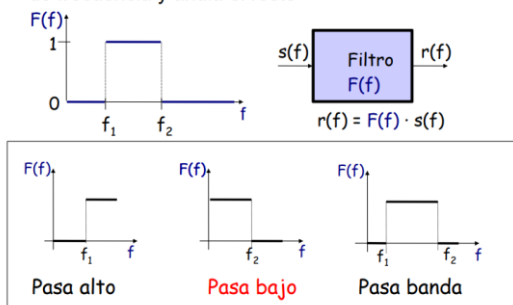
- La diferencia entre la componente espectral de mayor frecuencia y la de menor frecuencia es el ancho de banda de la señal.
- Las señales digitales tienen espectro infinito
  - La energía de la señal disminuye rápidamente al alejarnos de la frecuencia fundamental
  - Podemos aproximar razonablemente una señal a otra con ancho de banda finito

**Perturbaciones en la transmisión:**

- En su recorrido a lo largo del medio de transmisión, la señal sufre una serie de perturbaciones que degradan su calidad:
  - Ancho de banda limitado
  - Atenuación
  - Distorsión por atenuación y por retardo
  - Ruido

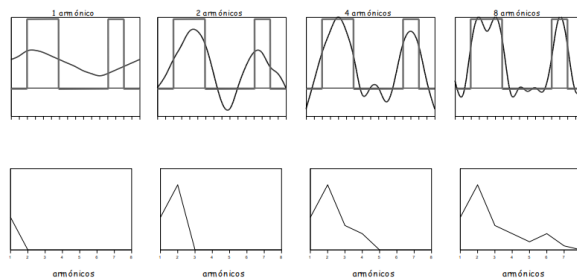
**Filtros**

- Dispositivo que deja pasar un rango de componentes de frecuencia y anula el resto

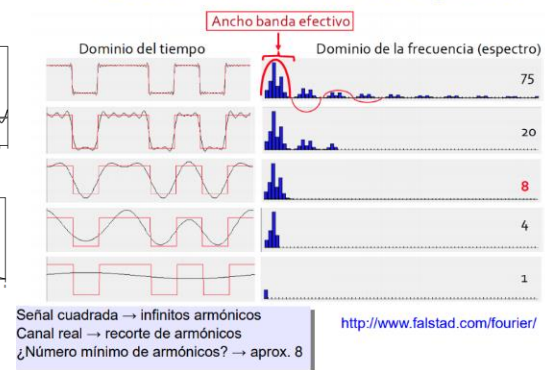
**Ancho de banda limitado**

- Los medios de transmisión se comportan como un filtro **pasa bajo**
- Este efecto limita la máxima frecuencia que puede atravesar el medio ( $f_2$ )
- El rango de frecuencias a las que permite el paso  $[0...f_2]$  es el **ancho de banda del medio**
- Existe una relación entre la **velocidad de transmisión** y el **ancho de banda del medio**

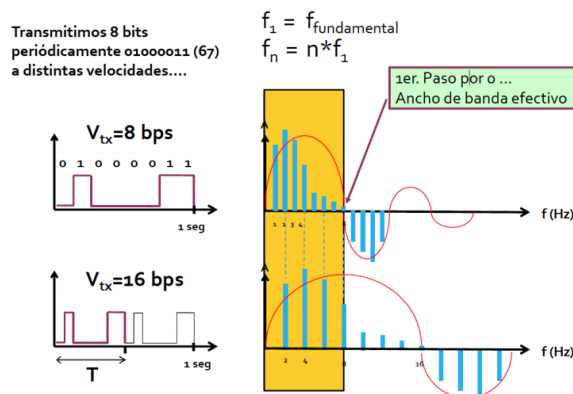
## Efecto sobre señales digitales



## Efecto sobre señales digitales

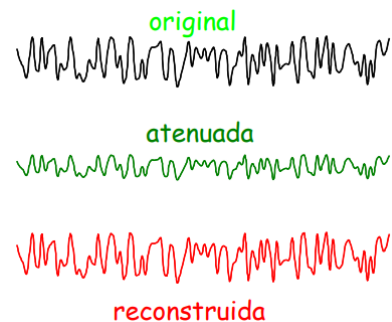


## Velocidad vs ancho de banda



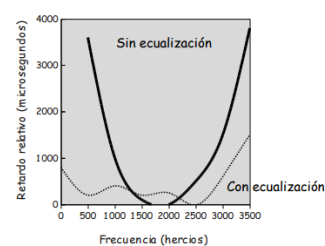
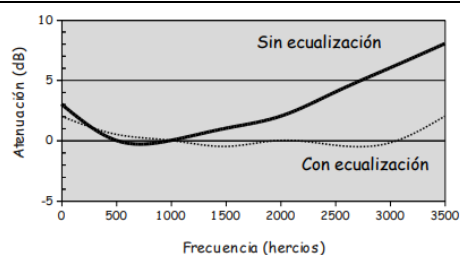
## Atenuación:

- Se trata de un efecto proporcional a la distancia recorrida
- Se puede compensar mediante:
  - Amplificadores (señal analógica)
    - También amplifican el ruido
  - Repetidores (señal digital o analógica que transporta datos digitales)



## Distorsión:

Distorsión por atenuación	Distorsión por retardo
<ul style="list-style-type: none"> <li>• La atenuación es creciente con la frecuencia</li> <li>• Las señales cambian su forma al atenuarse desigualmente sus armónicos</li> <li>• Se resuelve ecualizando la señal</li> </ul>	<ul style="list-style-type: none"> <li>• En medios guiados, la velocidad de propagación depende de la frecuencia</li> <li>• Las distintas componentes de la señal no llegan a la vez: se produce la distorsión por retardo</li> </ul>

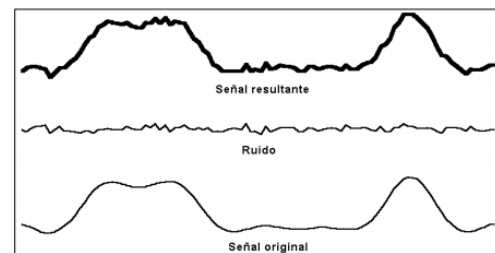


**Ruido:**

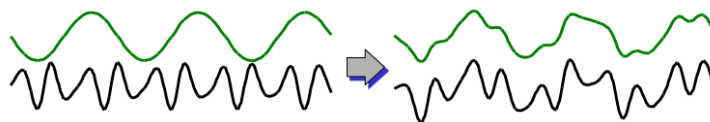
- El ruido corresponde a señales no deseadas que se inducen en la transmisión entre el emisor y el receptor.
- Factor de importancia a la hora de limitar las prestaciones en un sistema de comunicación.
- Según el origen:
  - Ruido térmico
  - Diafonía
  - Ruido impulsivo

**Ruido térmico:**

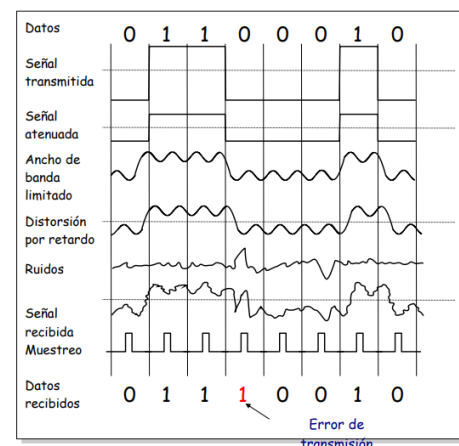
- Debido a la agitación térmica de los electrones dentro del conductor.
- Es función de la temperatura e independiente de la frecuencia (ruido blanco).
- No se puede eliminar: impone un límite superior a las prestaciones.

**Diafonía:**

- Causado por el acoplamiento no deseado de dos líneas adyacentes:
  - Aparece en la señal transmitida una porción de la señal transmitida en el otro canal.

**Ruido impulsivo:**

- Picos irregulares de corta duración y de amplitud relativamente grande.
- No es predecible, ni continuo.
- Se genera por:
  - Perturbaciones electromagnéticas.
  - Fallos y/o defectos en el sistema de comunicación.
- Es una de las principales fuentes de error en la comunicación digital de datos.

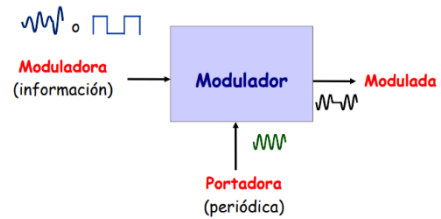
**Codificación y modulación:**

En ocasiones es necesaria una transformación de la señal, que transporta la información, para enviarla por el medio de transformación:

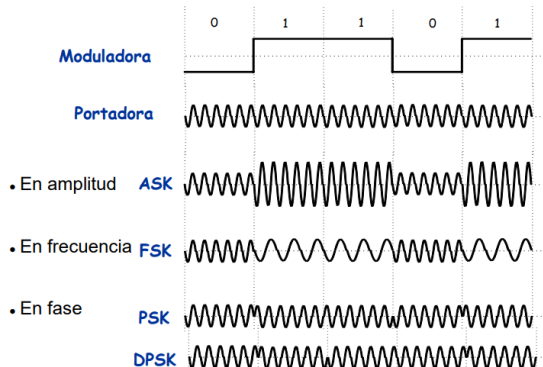
- Modulación: Genera una señal analógica a partir de una señal digital (o analógica).
- Codificación: Genera una señal digital a partir de otra digital.

**Modulación:**

- En el receptor se hace el proceso inverso (demodulación)

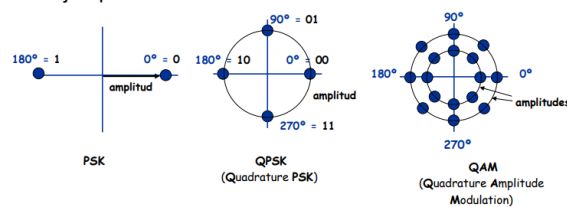


Banda base	Banda ancha
<ul style="list-style-type: none"> <li>La señal se transmite sin más, sin modular.</li> <li>Utiliza TODO el ancho de banda del canal.</li> <li>Multiplexación en el tiempo (TDM).</li> </ul>	<ul style="list-style-type: none"> <li>Mediante modulación (+ filtraje) se hacen subcanales en el canal.</li> <li>Multiplexación en frecuencia (FDM).</li> </ul>

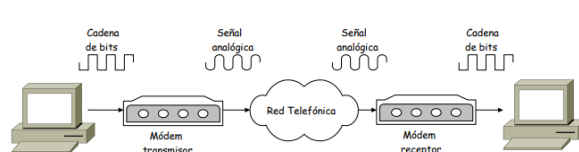
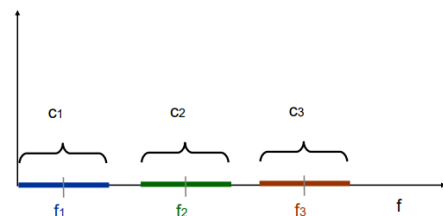
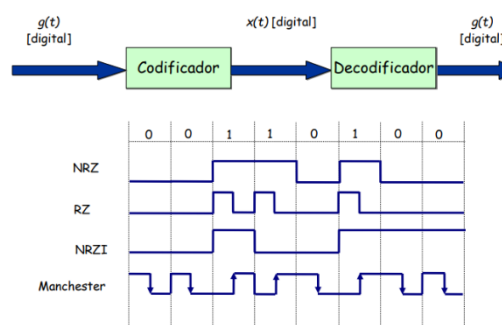
**Tipos de modulación****Modulación de múltiples niveles**

- Para conseguir mayores velocidades de transmisión podemos utilizar combinaciones de diferentes **amplitudes** y **fases**

- Ejemplos:

**Aplicaciones de la modulación:**

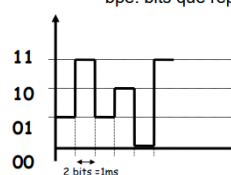
- Desplazamiento del espectro de una señal (limitada en banda) hacia otra zona del espectro
  - Transmisión de diversas señales por el mismo medio.
- Conversión de señales digitales a analógicas para adaptarlas a las características de la transmisión.
  - Fibra óptica.
  - Red telefónica conmutada

**Codificación**

- Velocidad de Transmisión:** número de bits transmitidos por unidad de tiempo (**bits por segundo, bps**)
- Velocidad de Modulación:** número de cambios que se generan en la señal por unidad de tiempo (**baudios**)

$$V_{mod} = V_{tx} / bpe$$

bpe: bits que representa cada elemento de la señal



$$V_{tx} = 2000 \text{ bps}$$

$$bpe = 2$$

$$V_{mod} = V_{tx} / 2 = 1000 \text{ baud}$$