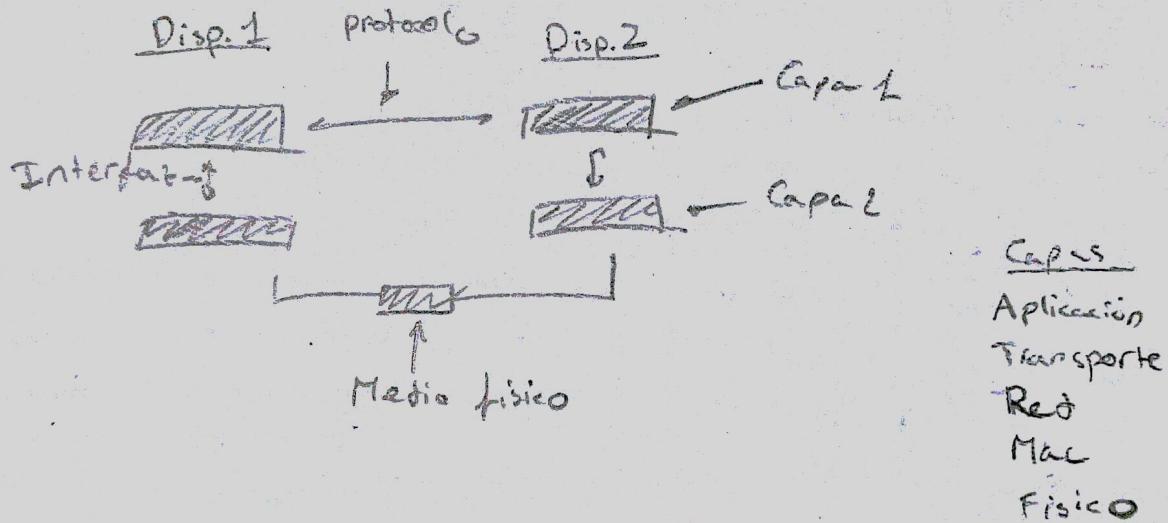


Servicio: Conjunto de funciones.

Protocolos: Reglas que gobiernan comunicación entre entidades de una misma capa en varios dispositivos.

Interfaz: Reglas que gobiernan comunicación entre entidades de distintas capas en un mismo dispositivo.



TCP/IP

Aplicación

Transporte

Red

Enlace (Host-Red)

Físico

OSI/ISO

Aplicación

Presentación

Sesión

Transporte

Red

Enlace

Físico

PDU: (Protocol Data Unit): Unidad de datos de protocolo

IDU: (Interface Data Unit): Unidad de datos de la interfaz

ICI: (Interface Control Information): Información de control de la interfaz

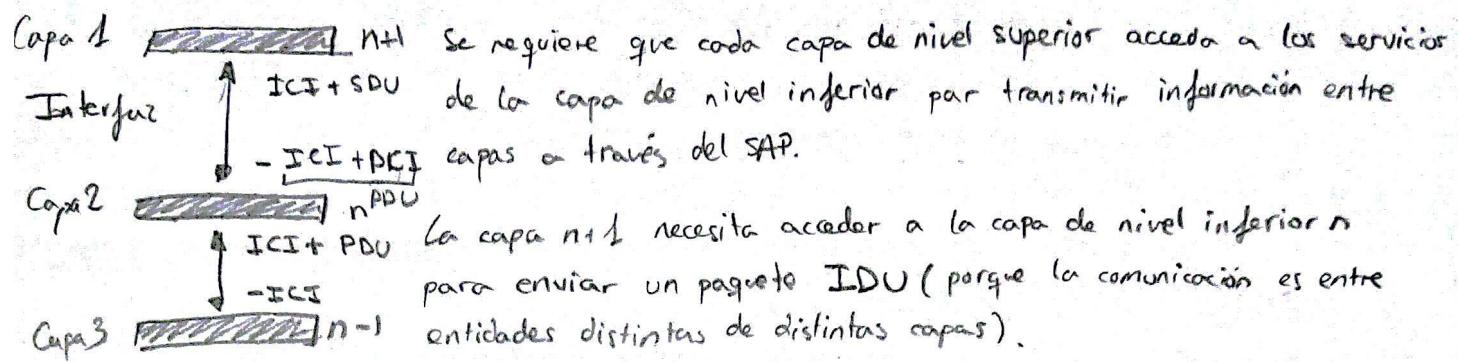
SDU: (Service Data Unit): Unidad de datos del servicio

SAP: (Service Access Point): Punto de acceso a servicios. → Identificador Único

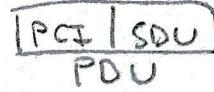
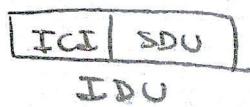
PCI: (Protocol Control Information): Información de control del protocolo

Flujo de información vertical

Dispositivo 1



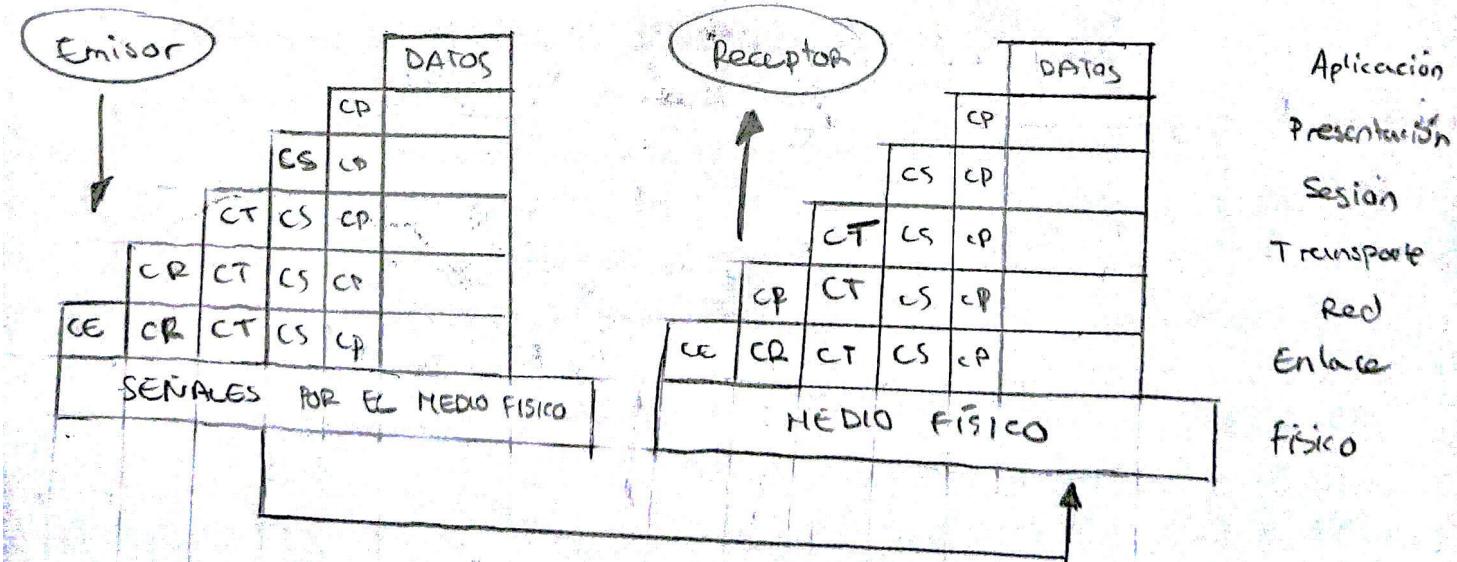
La IDU que se recibe en el nivel n se compone de 2 unidades de datos, la SDU del nivel n+1 y la ICI que ha añadido el mismo nivel n+1 antes de enviarla al nivel n.



Cuando la capa n recibe el IDU, elimina el ICI de la capa n+1 para quedarse con la SDU, a la que se le añade la cabecera PCI propia de la capa n. Este nuevo bloque constituye la PDU de la capa n.

Si se quisiera transmitir la información de la capa n a la n-1 se le añadiría la ICI de la capa n a la PDU de esa capa. Es decir la PDU de la capa n es la SDU de la capa n-1, repitiendo el proceso hasta alcanzar la capa de más bajo nivel.

La SDU de la capa inicial son los datos que se quieren enviar/reibir



Tema 2: Géneros (Transmisión de señales)

RTC: Red Telefónica Comutada

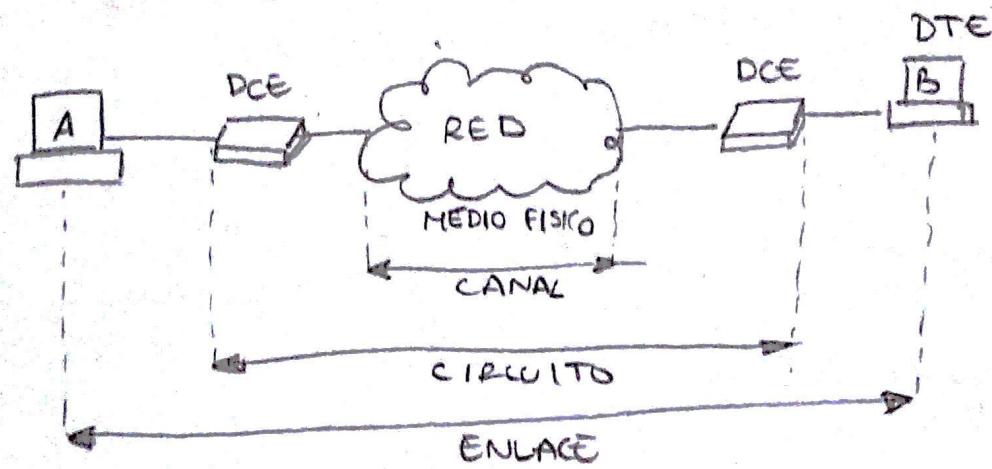
DTE: (Data Terminal Equipment): Equipo terminal de Datos, el que quiere enviar o recibir información (solicitante de servicio).

DCE: (Data Communicator Equipment): Equipo Comunicador de Datos, el que adapta los datos del DTE para poder ser transportada por el medio físico. (Ej: módem)

Canal de Datos: define una transmisión unidireccional en el medio físico.

Circuito de Datos: Define la comunicación entre los dos DCE.

Enlace de Datos: Define la comunicación entre los dos DTE.



SEÑALES POR SU NATURALEZA

- 1 [Análogica: Continua, varía suavemente en tiempo y amplitud.
- 1 [Digital: Discreta, sólo toma un número definido de valores en instantes determinados.
- 2 [Periódica: Formada por un patrón que se repite periódicamente.
- 2 [Aperiódica: no posee ningún patrón repetitivo.
- 3 [Simples: Basadas en funciones seno y coseno.
- 3 [Compuestas: Basadas en una composición de señales simples.

Tanto en los grupos 1, 2 y 3, si una señal es de un tipo no puede ser del otro, ya que sus definiciones son completamente opuestas.

Ancho de banda (B): Rango de frecuencias de las señales que se pueden transmitir por el medio (Hz).

- Mientras más pequeño sea el orden del armónico, mayor será la potencia.
- Debido al ancho de banda limitado, sólo se podrán transmitir los armónicos con frecuencia menor o igual a B.
- A mayor ancho de banda, más sencilla de reconstruir será la señal recibida.

Ganancia: Relación entre la amplitud de salida (V_s) y la de entrada (V_e), las dos de ellas son tensiones.

- La ganancia siempre cumple $G \leq 1$, ya que una ganancia de 1 es lo ideal para todos los armónicos.

$$G = \frac{V_s}{V_e}$$

↑
puede ser tanto la tensión como la Amplitud

$$G(\text{dB}) = 20 \log G = -3 \text{ dB}$$

$$\log G = \frac{-3}{20}$$

logaritmo en base 10

$$G = 10^{\frac{-3}{20}}$$

$$G = 0.707$$

Atenuación

la fórmula es también aplicable a la atenuación

$$\boxed{\text{Atenuación} = \frac{1}{\text{Ganancia}}}$$

Velocidad de Modulación (V_m): Véces por segundo que una señal puede cambiar su valor.

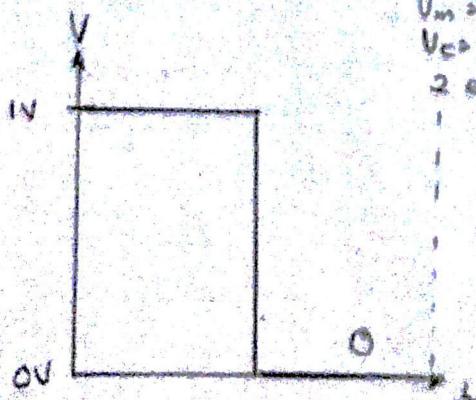
$$V_m = \frac{1 \text{ seg}}{0.1 \text{ seg}} = 10 \text{ baudios}$$

↑
periodo en el que cambia el valor

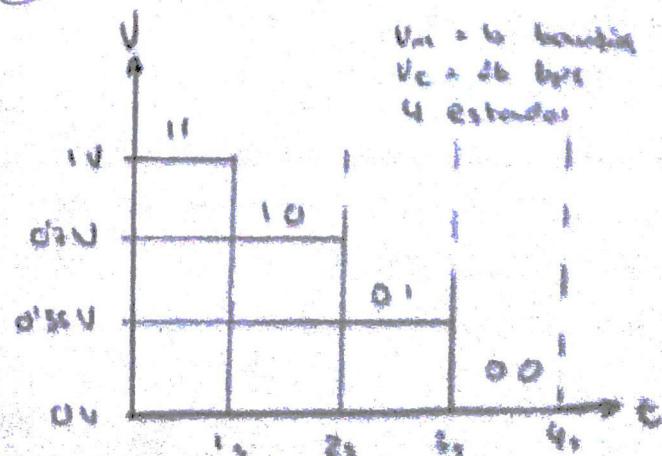
Velocidad de transmisión: Se mide en bits por segundo e indica cuantos bits de datos puede transmitir al mismo tiempo.

$$V_t = \frac{n \text{ bits}}{\text{tiempo}} = \text{bps}$$

$$V_t (\text{bps}) = V_m \cdot \log_2(N) = n^{\circ} \text{ estados significativos de la señal}$$



V_m = 10 baudios
 V_t = 1 bps
2 estados



$V_m = 10$ baudios
 $V_t = 26$ bps
4 estados

Considerando un total de λ bits transmitidos en T segundos la velocidad de transmisión será de:

$$V_e = \frac{\lambda}{T} = \lambda \cdot f_0 \rightarrow f_0 = \frac{V_e}{\lambda}$$

$$n \cdot f_0 \leq B \rightarrow n \cdot \frac{V_e}{\lambda} \leq B \rightarrow n \leq \frac{\lambda \cdot B}{V_e}$$

n = cantidad de armónicos

B = ancho de banda

V_e = Velocidad de transmisión

λ = Bits transferidos

Atenuación: Se mide en decibelios

$$\text{Ruido: } \left(\frac{P_s}{P_n} \right)_{dB} = 10 \log_{10} \frac{P_s}{P_n}$$

$\rightarrow A(dB) = 10 \log_{10} \frac{P_s}{P_e}$ → Potencias de entrada y salida

$\rightarrow V(dB) = 20 \log_{10} \frac{V_s}{V_e}$ → Tensiones de entrada y salida

$\frac{P_s}{P_n} = \frac{\text{Potencia de Señal}}{\text{Potencia de Ruido (Noise)}}$

↑
relación señal-ruido (dB) → cuanta más alta sea mejor transmisión

Teorema de muestreo (Nyquist)

periodo de muestreo $T_m = \frac{1}{2B}$ Una señal se puede reconstruir con muestras tomadas a una frecuencia de $2B$.

A partir de $f_m = 2B$ no se consigue mayor calidad, porque el medio elimina las componentes de alta frecuencia, es decir las que están por encima de B .

Velocidad máxima (según Nyquist)

$$V_{m MAX} = \frac{1}{T_m} = 2B$$

Considerando un medio sin ruido y N niveles o estados, la velocidad máxima teórica a la que se puede transmitir en un medio con ancho de banda B ps:

$$V_e (\text{bps}) = 2B \log_2 N$$

Velocidad máxima (según señal-ruido)

$$V_t \text{ (bps)} = B \log_2 \left(1 + \frac{P_S}{P_N} \right) = B \cdot \underbrace{\log_{10} \left(1 + \frac{P_S}{P_N} \right)}_{\log_{10} 2}$$

para hacerlo con la calculadora

donde $\frac{P_S}{P_N}$ no se expresa en decibelios y:

$$\left(\frac{P_S}{P_N} \right)_{dB} = 10 \cdot \log_{10} \left(\frac{P_S}{P_N} \right)$$

NO DECIBELIOS !!

Nyquist \geq Shannon (señal-ruido)

Puede que Nyquist no se alcance si supera el límite máximo establecido por Shannon. Ésto se debe a que por culpa del ruido los niveles de la señal serían irreconocibles.

Tema 3: Codificación de la información

Codificación en Banda Base

Unipolar: Cuando todos los niveles de amplitud se encuentran a un mismo lado del eje de tiempo, es decir, o todos los valores son mayores o iguales a cero, o todos son menores o iguales a cero.

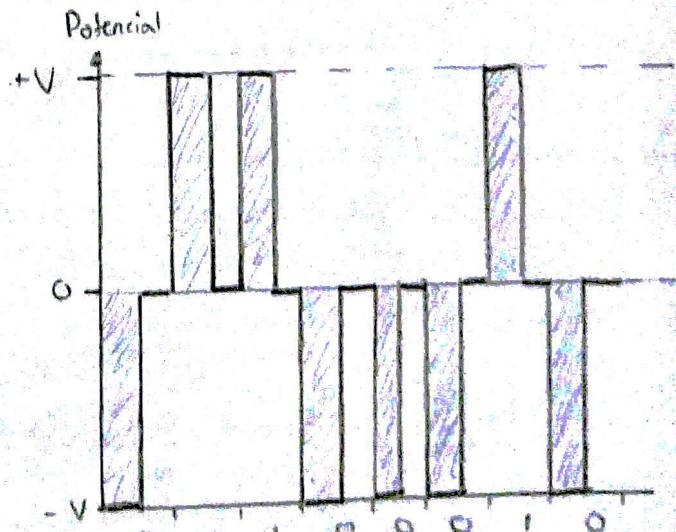
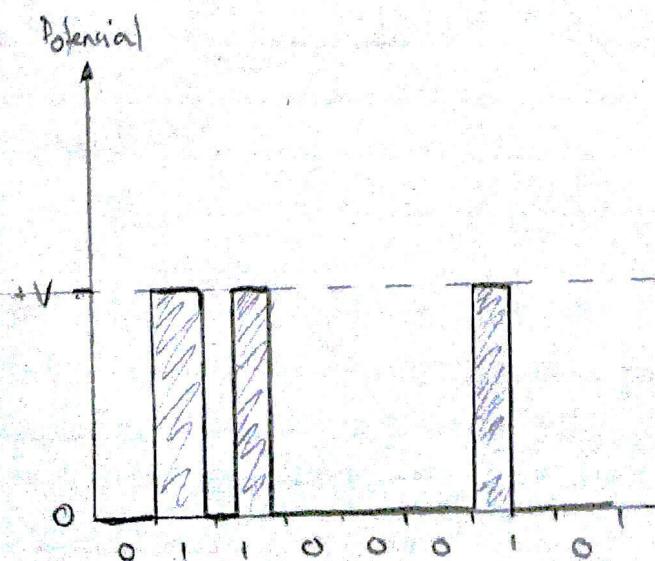
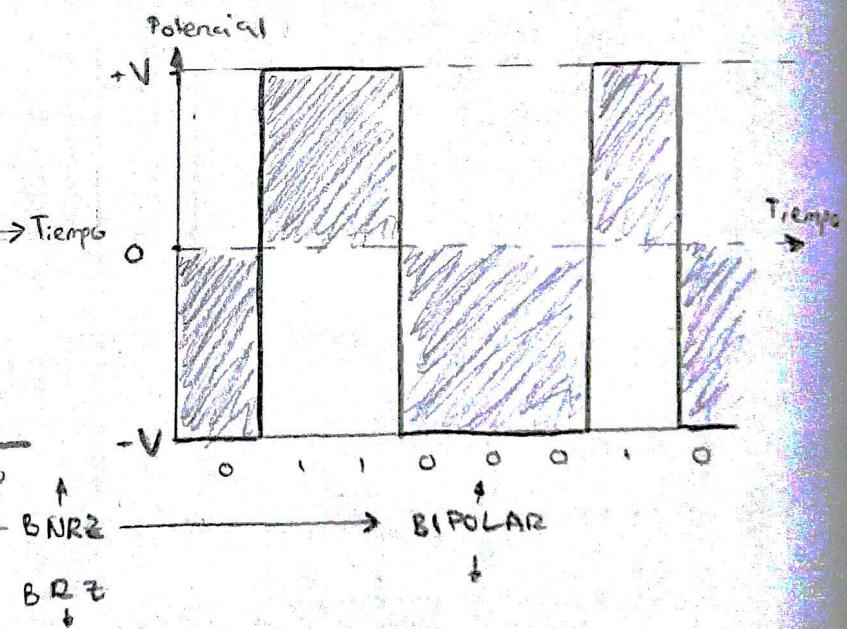
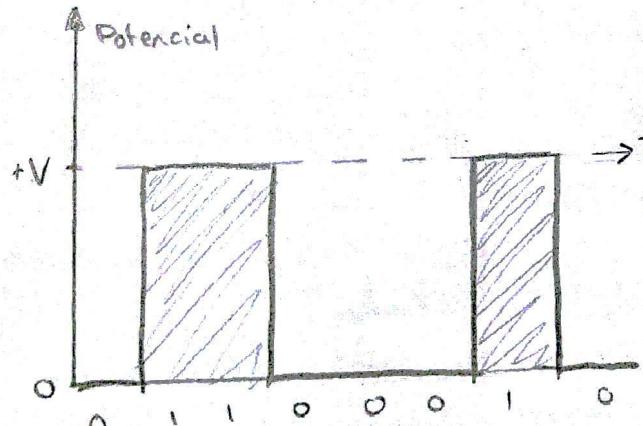
Bipolar: Cuando los niveles de amplitud se pueden encontrar a ambos lados del eje del tiempo.

Multinivel: Cuando en la señal se pueden tener diferentes tipos de elementos de señal



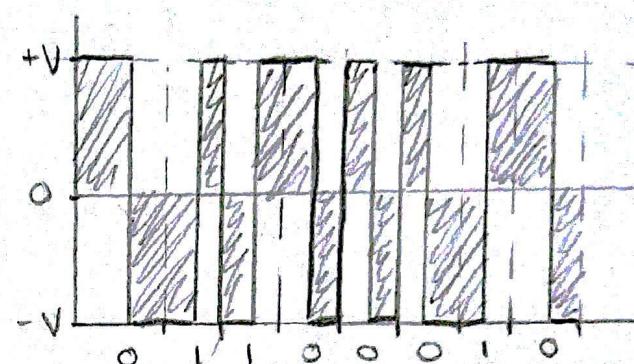
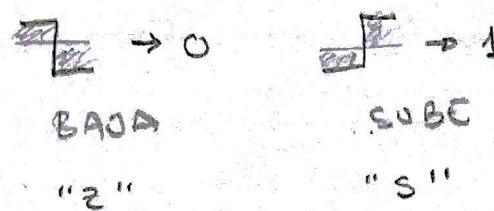
Codificación Binaria

- Se asignan niveles de tensión a cada valor del bit (0 o 1).
- Codificación BRZ (binaria con Retorno a Zero) y BNRZ (sin retorno a zero) diseñadas como unipolares



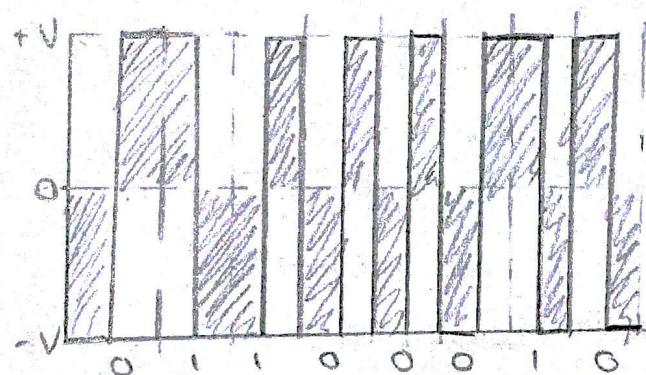
Manchester

Pertenece a la codificación bipolar y se le asignan transiciones de tensión a los bits 0 y 1.



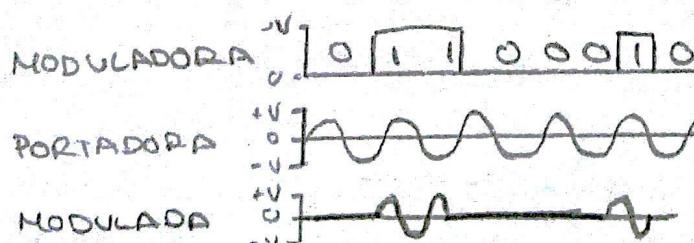
Manchester Diferencial

La transición de tensión cambia si se encuentra un 1, si se encuentra un 0 se continua con la transición actual



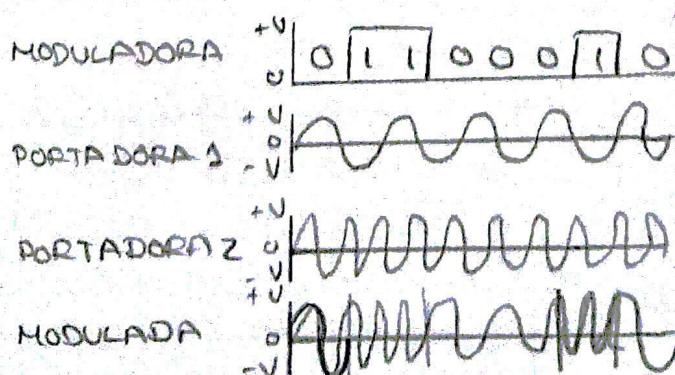
Codificación Banda Modulada

ASK (Amplitude Shift Keying)

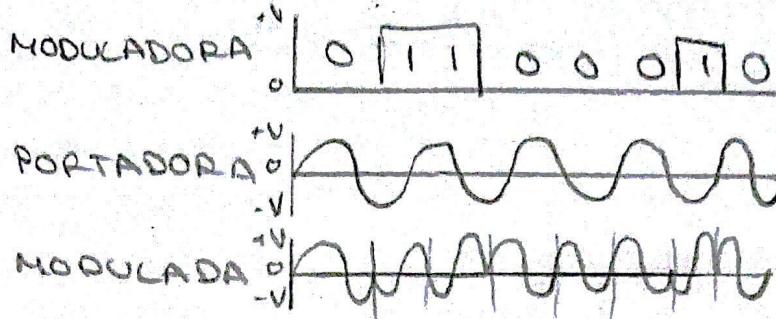


NO NECESARIAMENTE TIENE QUE SER Amplitud ϕ

FSK (Frequency Shift Keying)



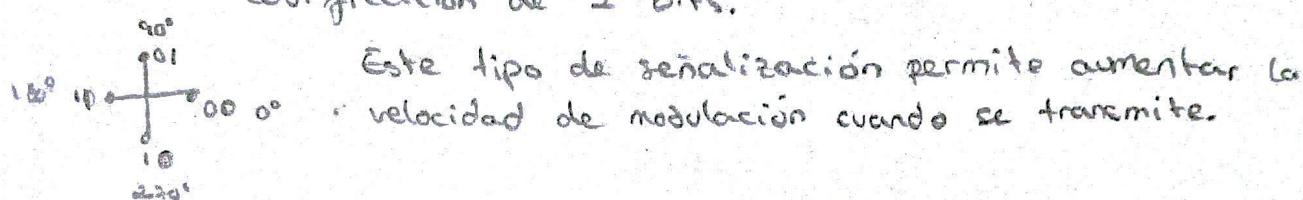
PSK (Phase Shift Keying)



El cuadro cambia la fase se especifica en la fórmula.

Si encuentra un número diferente cambia de fase, sino continúa con la actual.

QPSK: Es una variación de PSK en el que la fase permite la codificación de 2 bits.



QAM: Es una variante tanto de ASK como de PSK en el que se emplean distintas amplitudes y desplazamientos de fase de la señal portadora. (Quadrature Amplitude Modulation)

MODULACIÓN DIGITAL (Digitalización de información)

PCM (Modulación por codificación de pulsos)

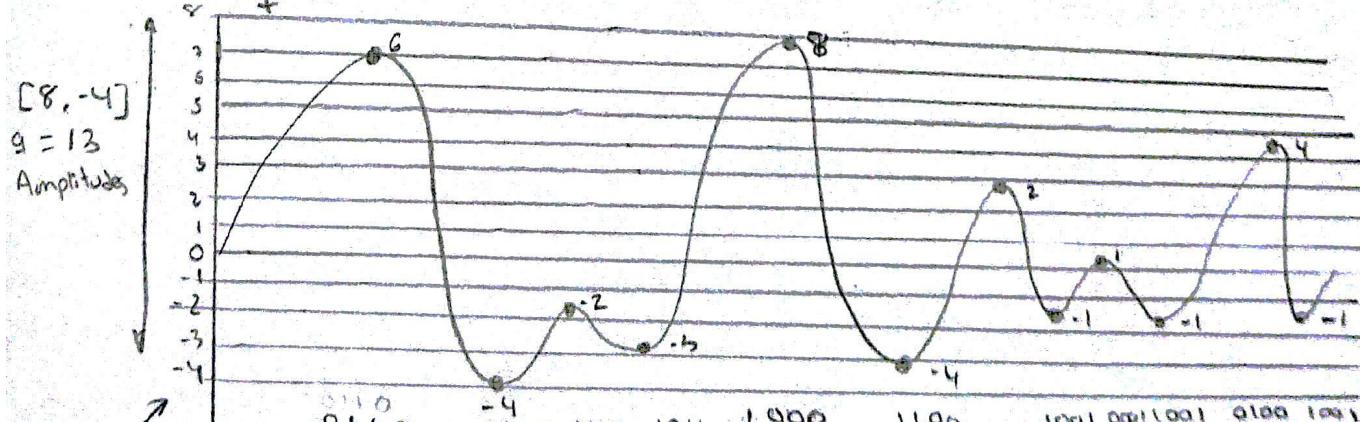
(Pulse Code Modulation)

Frecuencia de muestreo $\rightarrow f_m = 2B \rightarrow$ según Nyquist

$q = n$ º niveles de cuantización (incremento constante)

$n = n$ º bits necesarios para codificar los niveles q .

$$q = 2^n \rightarrow n = \log_2 q$$



supuestamente De la señal analógica se toman muestras cada cierto periodo deberíais tener de tiempo, se les asigna un valor y dicho valor se codifica. (por aproximación)
la misma amplitud hasta llegar al 0.

$$V_{T\text{-digital}} = \frac{n}{T_{m\text{-digital}}} = n \cdot f_{m\text{-digital}} = n \cdot 2B \text{ bps}$$

$$T_{m\text{-digital}} = \frac{T_{m\text{-señal}}}{n} \rightarrow f_{m\text{-digital}} = \frac{1}{T_{m\text{-digital}}} = \frac{n}{T_{m\text{-señal}}} = \frac{n}{\frac{1}{2B\text{señal}}} = 2B\text{señal} \cdot n \text{ Hz}$$

$$f_{m\text{-digital}} \leq 2B_{\text{digital}} \rightarrow n \cdot 2B_{\text{señal}} \leq 2B_{\text{digital}}$$

$$n \leq \frac{B_{\text{digital}}}{B_{\text{señal}}}$$

FDN (Multiplexión por división de frecuencias)

$$B_{\text{medio}} = n \cdot (B_{\text{canal}} + \Delta B) \text{ Hz}$$

$n = \text{nº canales a multiplexar}$

TDM (Multiplexión por división en tiempo)

Síncrona: Se asigna una posición temporal periódica para transmitir



Estadística: Cada fuente no tiene asignada una misma posición temporal periódica.

$$f_m = 2B$$

$$\begin{array}{ccccccc} & 1 & 2 & 3 & 3 & 1 & 2 & 3 & 2 \dots \\ \hline & 1 & 1 & 2 & 3 & 3 & 1 & 2 & 3 \end{array} \quad T_m = \frac{1}{f_m}$$

$$V_t = \frac{\text{bits sincro}}{T_m} \text{ bps}$$

$$V_{t\text{ canal multiplexado}} = \text{nº canales} \cdot V_t = V_{t_1} + V_{t_2} + V_{t_3} + V_{t_n}$$

pueden ser iguales o diferentes

Tema 4: Medios de Transmisión

Fibra Óptica

Ley de Snell

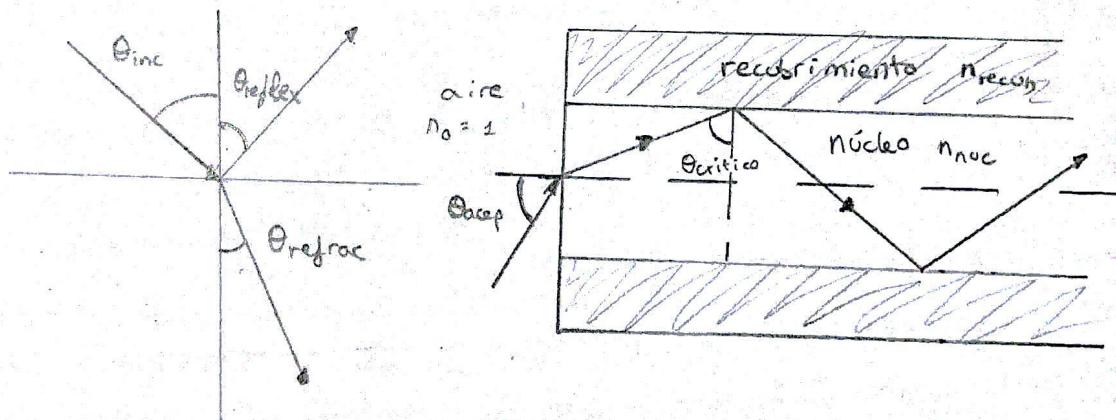
$$\text{índice de refracción del medio} \rightarrow n = \frac{v_0}{v_n} = \frac{\text{velocidad medio origen}}{\text{velocidad medio destino}}$$

↑
velocidad de
propagación de la luz

$$n_1 \cdot \sin \theta_{\text{incidente}} = n_2 \cdot \sin \theta_{\text{refractado}}$$

En el aire el índice de refracción es 1 $[n=1]$

$$\theta_{\text{crítico}} = \arcsen \left(\frac{n_{\text{recubrimiento}}}{n_{\text{núcleo}}} \right)$$



Tema 4 Diapositivas: Nivel de Enlace

Modelo 802 IEEE

Aplicación	Aplicación
Transporte	Transporte
Red	Red
Enlace	LLC
Físico	MAC
	Físico

LLC (Logic Link Control):

Control de Enlace Lógico que tiene la función de controlar el flujo de datos y de controlar los errores.

MAC (Medium Access Control):

Control de Acceso al Medio. Tiene funcionalidades de reparto del medio físico, direccionamiento físico, etc.

Modelo TCP/IP

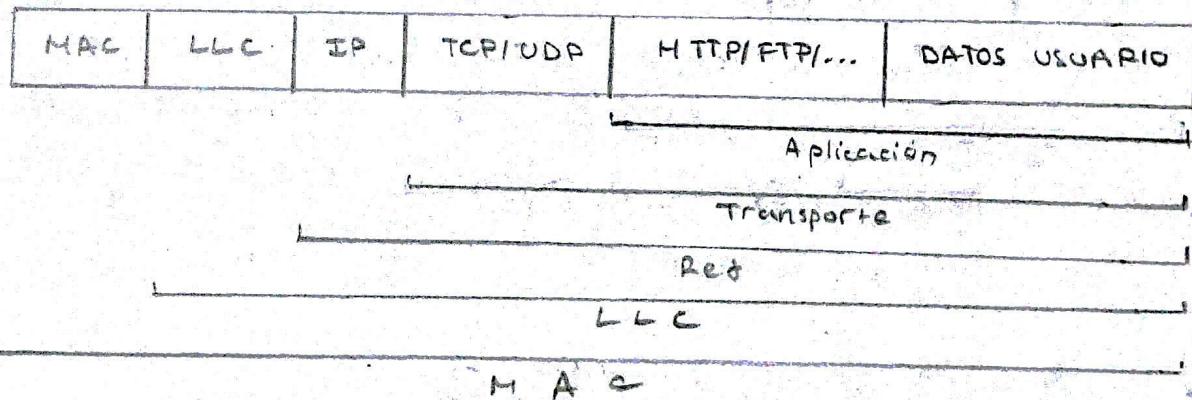
+

Modelo OSI

Modelo TCP/IP

+

Modelo 802 IEEE



LLC se basó en el protocolo HDLC (Protocolo de Control del Enlace de Alto Nivel) proporcionando 3 tipos de servicio al nivel superior, es decir 3 mecanismos para el envío de paquetes del nivel de Red (IP):

Tipo 1 - Sin conexión, sin confirmación: Es el empleado por TCP/IP y es el más rápido en funcionamiento ya que no controla ni errores ni flujo. (Tipo 1)

Tipo 3 - Sin conexión, con confirmación: Confirma la llegada de paquetes, es decir, controla los errores. (Tipo 3)

Tipo 2 - Con conexión: Controla tanto errores como flujo, aunque es más lenta. (Tipo 2)

LLC está implementado en los trivers del dispositivo de comunicación (tarjetas de red) que emplea las normativas IEEE 802.

DSAP	SSAP	Control LLC	Código de Protocolo	Tipo paquete EtherType	DATOS (IP/ARP)
1 byte	1 byte	1 byte	3 bytes	2 bytes	

Cabecera LLC

DSAP: Punto de Acceso al Servicio de Destino.

SSAP: Punto de Acceso al Servicio de Origen. } En TCP/IP tienen 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 TCP/IP tiene asociado el valor 0.

Tipo Paquete: Los paquetes IP tienen asociados el valor 2048 (0x0800), y los paquetes ARP el 2054 (0x0806).

Ethernet CSMA/CD, Comunicación y Puertos

- Una red Ethernet se caracteriza por emplear un medio físico compartido entre todas las estaciones con topología de BUS.
- Las redes Ethernet, debido a la necesidad de compartir el medio físico, son semidúplex y emplean un mecanismo CSMA/CD para el reparto del medio.
- Las diferentes versiones tecnológicas se denominan empleando la nomenclatura:

Velocidad - Señalización - Medio físico

- Velocidad: 10 (Mbps), 100 (Mbps), 1000 (Mbps), 10G (Gbps)
- Señalización: Base (banda base, Manchester), o Broad (Banda Modulada)
- Medio físico: T (UTP), C (STP), F (Fibra óptica), X (varios medios físicos)

{ 10 Base 2 : De las primeras Ethernet que usaban coaxial fino. 10 Mbps a 185 m.

10 Base 5 : Coaxial grueso (Categoría 5), 10 Mbps hasta 500 m.

Desaparecen del mercado con la introducción de los UTP (mayor tolerancia a fallos, facilidad de implantación y mejoras prestacionales [y precio]).

IEEE 802.3

Preámbulo	SFD	MAC Destino	MAC Origen	Longitud	LLC	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	4 bytes	4 bytes 46-1500 bytes

MTU (Maximum Transfer Unit): es el máximo tamaño de paquete que se puede transferir en una red.

El MTU en una red 802.3 es de 1492 bytes

Preámbulo: Secuencia de 7 bytes (0101010)

SFD: Delimitador de trama (0101011)

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.

Ethernet II

Ethernet Digital / Intel / Xerox (Ethernet DIX), también conocida como Ethernet II no emplea la capa LLC y permite la introducción del datagrama IP en el paquete de nivel MAC.

Preámbulo	MAC Destino	MAC Origen	Tipo	Datagrama IP	Relleno (opcional)	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes		4 bytes

El MTU (tamaño máximo del paquete IP) en una red Ethernet DIX es 1500 bytes

Este es el formato que se emplea en redes TCP/IP.

Preámbulo: Equivalente al campo Preámbulo + SFD del IEEE 802.3

Tipo: Código para identificar el protocolo del contenido del paquete MAC (ARP/IP)

Tipo = 0x0800 . Protocolo IP

Tipo = 0x0806 . Protocolo ARP

CSMA/CD

- Tanto IEEE 802.3 como Ethernet DIX utilizan el mecanismo CSMA/CD para compartir el bus común. Este mecanismo consiste en comprobar el medio físico antes de transmitir un paquete de datos en un medio que SIEMPRE ES SEMIDUPLEX.
- su principal problema está en la comprobación y transmisión simultánea de datos por 2 o más estaciones.



- Para asegurar que dos estaciones que transmiten simultáneamente detectan la colisión, es necesario que la transmisión dure lo suficiente para llegar al otro extremo.
- En Ethernet la extensión máxima de la red (con repetidores) es 2'5 Km (5 buses 10Base5).
- En una red a 10Mbps y 2'5 Km de extensión, el tiempo mínimo de transmisión necesario son 512 tiempos de bit, es decir un paquete ethernet de 64 bytes (46 de datos sin tener en cuenta el prefámbulo)
- Al tiempo mínimo de transmisión se lo denomina ranura temporal.

Algoritmo CSMA/CD. Transmisión

1. Escucha el medio antes de transmitir.

2. 96 tiempos de bit de espera $T_{espera} = \frac{96}{10.000.000} = 9'6 \mu\text{segundos}$

3. Transmisión del paquete escuchando el medio. 10 Mbps

4. Cuando la tensión de la señal es anómala, debido a la superposición de señales, se detecta una colisión.

5. Si se detecta colisión, se envía una señal JAM (señal de congestión) para reforzarla.

6. Si el paquete no llega correctamente se reenvia hasta un total de 16 intentos.

7. En cada intento, se espera un número aleatorio de veces el tiempo de ranura (regresión exponencial).

8. El tiempo de ranura se determina como el doble del tiempo que tarda un bit en propagarse en la red ethernet ($512 \mu\text{segundos}$)

Recepción

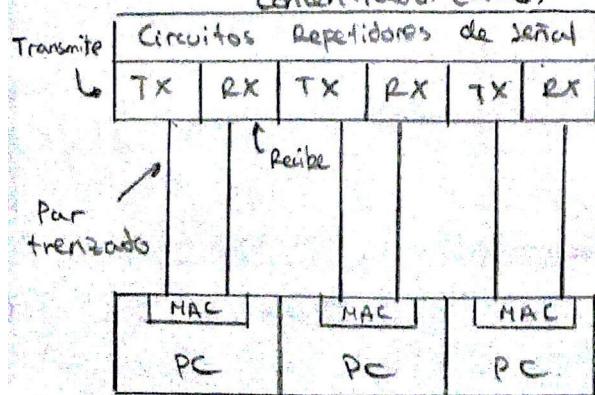
1. El prefámbulo permite sincronizar el receptor con la trama a leer (modo asíncrono).

2. La interpretación del campo dirección destino en la trama es inmediata.

Concentrador Ethernet (HUB)

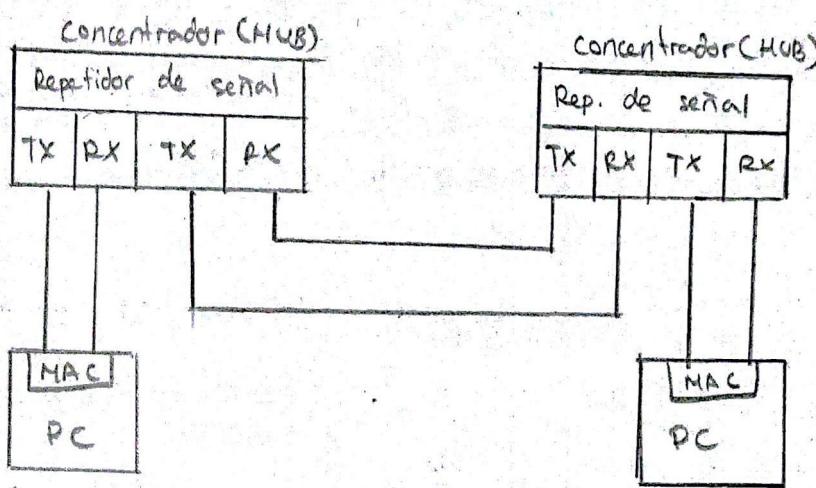
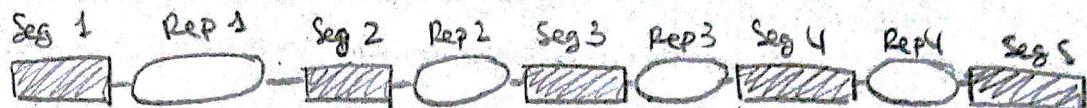
La red 10 BaseT emplea topología en estrella, donde el elemento central se denomina concentrador o hub.

(concentrador (HUB))



- Las colisiones se detectan cuando se recibe la señal por el par de recepción al mismo tiempo que se transmite la trama.
- Detección de problemas en cableado más fácil que con coaxial
- Distancia máxima entre equipo y concentrador debe ser inferior a 100 m
- La red ethernet puede crecer interconectando concentradores con cables UTP cruzados (repetidores)

El número máximo de HUB's que pueden colocarse en cascada está limitado por la extensión máxima de una red Ethernet (2^5 Km) por lo que en 10 Base 5 serían 5 segmentos entre los que hay 4 repetidores.



Dominio de colisión: Dispositivos en una red que pueden colisionar al transmitir simultáneamente

- El hub tiene el inconveniente de que aumenta la probabilidad de colisiones al ser mayor el dominio de colisión.

Puentes

- Con los puentes o Bridges se reduce el número de colisiones, ya que dicho dispositivo analiza la cabecera MAC de los paquetes para determinar si hay que reenviarlos o no de un segmento a otro.
- Los puentes dividen la red en segmentos de colisión independientes, por lo que las LAN interconectadas con puentes no tienen limitación de extensión al crecer.
- Los puentes transparentes son aquellos que deciden cómo se intercambian los paquetes entre segmentos, es decir, que los equipos no conocen la estructura de la red.
- Estos puertos transparentes poseen una CPU que controla su funcionamiento, buffers de E/S donde se almacenan las tramas en proceso (FIFO) → cola, y una base de datos, que no es más que una tabla de asociación de direcciones MAC con números de puerto (tabla de reenvío).
- Un puente lee todos los paquetes recibidos por un puerto (modo promiscuo) y los almacena en un buffer para procesarlos.
- Un puente trabaja en dos modos simultáneamente: modo de reenvío y modo de aprendizaje.

Modo de reenvío

- Se comprueba la MAC destino de cada paquete Ethernet que llega a un puerto.
- Si la dirección está en la tabla de reenvío, se reenvía el paquete al puerto asociado (siempre que el puerto asociado sea distinto al puerto al que ha llegado el paquete).
- Si la MAC destino no existe en la tabla de reenvío, el paquete se reenvía a todos los puertos excepto por el que se recibió.
- Los paquetes cuya dirección destino sea la dirección de Broadcast se reenvian a todos los puertos, excepto al puerto por el que se recibió el paquete de difusión.

Modo de aprendizaje

- Se comprueba la MAC origen de cada paquete Ethernet que llega a un puerto.
- Si la MAC 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 aprendizaje, dado que no se conocen las MAC de los equipos, la mayor parte de los paquetes son reenviados por todos los puertos, por lo que los demás puertos aprenderán información. A este fenómeno se le conoce como inundación.
- Cada entrada de la tabla de reenvío de un puente tiene asociado un temporizador en segundos que mide el tiempo desde que se creó la entrada en la tabla.
- Si se recibe un paquete con una MAC origen por el puerto que se indica en la tabla de reenvío, el temporizador se inicializa a 0.
- Si el temporizador alcanza un determinado valor máximo, la entrada de la tabla de reenvío se elimina. De esta forma las tablas se ajustan a cambios en la estructura de la red.
- Este modo de aprendizaje requiere que la LAN con puentes tenga una estructura de árbol simple de expansión.

Algoritmo de árbol de Expansión

- Cada puente determina un coste RPC (nº redes intermedias, velocidad de transmisión) desde cada puerto al puente raíz, que será el identificador más bajo de uno de los puentes del árbol. Al puerto con menor coste se le denominará puerto raíz del puente.
- En cada puente se elige un puerto designado, que es el puerto con menor valor RPC conectado al puente.
- Finalmente se activan todos los puertos raíz y designados de la red, obteniendo una estructura de árbol.

Ethernet Commutada

Con el uso de puentes se llegó a la posibilidad de construir un puente multipuerto donde se conectaría cada puerto, un equipo en vez de un segmento de red. Estos dispositivos son conocidos como comunicadores o switches definiendo las redes Ethernet commutadas.

Modo full-duplex: No existen colisiones (CSMA/CD no activo) y existe transmisión y recepción simultánea al no emplear la línea CD.

Modo half-duplex (semiduplex): Permite conexión de equipos con CSMA/CD (concentrador 10BaseT) y se emplea la línea CD.

Fast Ethernet

- Con el desarrollo de los comunicadores Ethernet el rendimiento se dispara si el tráfico tiene una distribución homogénea en la red, es por ello por lo que la mayor parte de las aplicaciones de red en entorno LAN siguen la arquitectura cliente/servidor.
- Para conseguir un acceso adecuado entre clientes y servidor, es necesario un puerto de mayor velocidad en el comunicador donde conectar el servidor, con un puerto a 100 Mbps, el servidor puede atender las peticiones y respuestas con 10 clientes a 10 Mbps de manera simultánea.
- La normativa que permite la transmisión de paquetes Ethernet a 100 Mbps se denomina de forma genérica Fast Ethernet, existiendo diversas modalidades para la transmisión.
- Para permitir el mismo tipo de protocolo MAC empleando diferentes tipos de medios físicos, se introdujo una estructura de subcapas para el nivel físico.

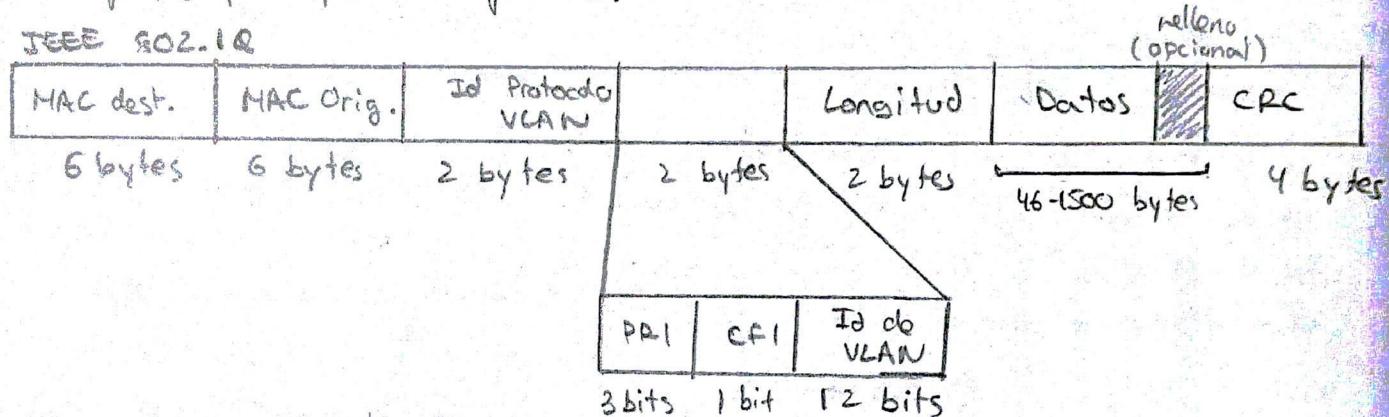
Subcapa de convergencia (CS): Convierte el flujo de la capa MAC en grupos de 4 bits para su envío a la subcapa PMD.

Subcapa dependiente del medio físico (PMD): Transmite cada grupo de 4 bits con el mecanismo de codificación adecuado a cada tipo de medio físico.

Redes Locales Virtuales (VLAN)

- El IEEE desarrolla una normativa (IEEE 802.1Q) para poder dividir un commutador en varios dominios de difusión distintos llamados VLAN (Virtual Local Area Network).
- Los commutadores VLAN funcionan de forma similar a un puente (bridge), disponiendo de una tabla de reenvío.
- Las tramas de difusión (broadcast) de entrada en un puerto se envían únicamente a los miembros pertenecientes a la misma VLAN.
- Si un equipo de una VLAN envía un paquete a una MAC de otra VLAN, el commutador no lo reenvía, ya que cada VLAN tiene asociada una IP de red diferente para que ARP funcione.

IEEE 802.1Q



Id Protocolo VLAN: Toma el valor 0x8100 para indicar que es un paquete IEEE 802.1Q.

PRI: Bits de prioridad que pueden emplearse para commutar unos paquetes antes que otros (voz, video).

CFI: Flag para indicar que en el campo de datos hay una trama Token-Ring.

- Los puertos troncales (trunk port) pertenecen a varias VLAN, y a través de ellos los paquetes de diferentes VLAN se intercambian entre commutadores distintos, todo esto es necesario hacerlo en el formato 802.1Q.
- Cuando un Enlace de Acceso, proveniente de un Equipo, envía un paquete a un enlace troncal, los paquetes en formato 802.3 provenientes del equipo se deben transformar a 802.1Q para poder transmitirlo entre commutadores.
- De igual modo, cuando un enlace troncal envía un paquete a un enlace de acceso se debe eliminar el identificador VLAN del enlace de acceso añadido anteriormente para transformarlo de formato 802.1Q a 802.3.
- Los commutadores VLAN utilizan un protocolo llamado GVRP (GARP VLAN Registration Protocol) para propagar información entre commutadores y conocer qué VLAN's hay asociadas a los puertos troncales, así el commutador sabrá automáticamente si debe reenviar paquetes a VLAN's de otros commutadores conectados por puertos troncales.

LAN Inalámbrica

BSS (Basic Service Set): Conjunto de servicio básico. Grupo de estaciones que se comunican entre ellas.

- Infrastructure BSS (IBSS): Red Inalámbrica con puntos de acceso (red de infraestructura)

- Independent BSS (IBSS): Red Inalámbrica ad-hoc.

- SSID (Service Set Identifier): Identificador de un BSS. Cada uno de 32 caracteres máximo.

- BSSID (Basic Service Set Identifier): SSID en redes ad-hoc.

- ESSID (Extended Service Set Identifier): SSID en redes de infraestructura.

AP (Access Point): Punto de Acceso inalámbrico a una red. Actúa como puente entre la LAN y un BSS.

Acceso al Medio

- Elevada tasa de error en el medio físico, lo que condiciona el mecanismo de reparto del uso del medio físico.

Al incrementarse la tasa de error en el medio, se introducen dos necesidades:

1. Es necesario un tamaño de paquete más pequeño, ya que los errores provocarán reenvíos más pequeños de datos. Los paquetes de nivel superior (L4C) serán fragmentados por el protocolo MAC del 802.11, la cual especifica un tamaño máximo de datos de 2312 bytes.

Control de trama	Id duración	Dirección 1	Dirección 2	Dirección 3	Nº secuencia	Dirección 4	DATOS	CRC
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	máximo 2312 bytes	4 bytes

Cabecera MAC IEEE 802.11x
30 bytes

2. 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 en el medio inalámbrico. Así, los reenvíos necesarios se realizarán rápidamente.

DCF (Función de Coordinación Distribuida)

- En este modo, cada estación compite por el uso del medio físico. El mecanismo de reparto es el CSMA/CA (Acceso al medio con detección de portadora y evitación de colisiones).
 - Las estaciones comprueban si el medio está libre detectando una señal CCA (Estimación de desocupación del canal), que transmiten los dispositivos en escucha en la red.
 - Si se encuentra el medio libre durante un tiempo DIFS (Espacio de tiempo entre la transmisión de tramas en DCF), entonces transmitirá el paquete del cual, si recibe una confirmación de envío, considerará como correctamente transmitido.
 - Si la estación detecta que el medio está ocupado, espera a que se detecte de nuevo el medio físico libre durante un tiempo DIFS. Al expiration este tiempo, el equipo entra en contienda esperando un tiempo aleatorio. Al terminar dicho tiempo aleatorio y si el medio esta libre, transmitirá, sino esperará un nuevo periodo de contienda, repitiendo el proceso tantas veces sea necesario.
- Para evitar el problema de la estación oculta (un AP que detecta 2 estaciones, pero las estaciones no se detectan entre sí), se introduce un mecanismo de reserva de la red, en el que se transmite un paquete RTS que indica al resto de estaciones "visibles" por el AP, el tiempo durante el que no pueden transmitir (NAV - Vector de reserva de red).
- El receptor confirma el RTS con un paquete CTS que indica al resto de "visibles" el tiempo durante el que no pueden transmitir.

PCF (Función de Coordinación Centralizada)

- Este modo únicamente funciona para redes de infraestructura, pues precisa de un punto de acceso AP:
 - Cuando existe un AP todas las comunicaciones se hacen a través de él.
 - El AP divide el tiempo de transmisión en la red en celdas de tiempo llamadas supertramas.
 - Cada supertrama se divide en 2 períodos de tiempo:
 - Un periodo en el que no hay colisiones y el AP controla el uso del medio para seleccionar los equipos a transmitir.
 - Un periodo de contienda donde se emplea CSMA/CA o CSMA/CA con RTS/CTS

Seguridad en redes WiFi

Principios

Autenticación: Una estación (cliente) debe identificarse como usuario autorizado de la red WiFi, existiendo diferentes mecanismos de autenticación.

Integridad de la información: La información debe transmitirse cifrada para evitar espías (sniffers).

Autenticación

- Para realizar el registro en una red WiFi, la estación debe conocer el SSID de la red, donde puede introducirse un mecanismo de seguridad.
- Los AP transmiten cada cierto tiempo su SSID en un paquete de señalización para invitar a equipos a unirse. Dicha acción puede deshabilitarse en el AP, de forma que los equipos no "ven" la red y solo pueden conectarse si conocen el SSID.
- Un nivel de seguridad adicional consiste en permitir solamente el registro de estaciones con la MAC almacenada en una lista del AP.
- Una vez finalizado el registro es posible llevar a cabo un proceso de autenticación.

CIFRADO WEP

- WEP (Wired Equivalent Privacy) fue el primer protocolo de encriptación empleado en el standard IEEE 802.11x hacia 1999 y se basa en el algoritmo de cifrado RC4.
- Su funcionamiento está basado en el conocimiento de una misma clave secreta por parte de la estación y el AP (PSK - Pre-Shared Key).
- El equipo o estación proporciona información cifrada al AP con la clave secreta y, si esta información es correcta, el AP permite la conexión de la estación a la red.
- Al estar basada en una clave de 64 a 128 bits, WEP está obsoleto pues es posible descubrir la clave en unos pocos minutos con el software apropiado.

CIFRADO WPA

- (WiFi Protected Access) WPA fue desarrollado por la Wi-Fi Alliance en 2003 para sustituir a WEP.
- WPA mantiene el algoritmo 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 (MIC - Message Integrity Code).
- Actualmente, el WPA basado en TKIP se ha roto, por lo que no es seguro emplearlo aunque se requieren unos 15 minutos para descubrir la clave. Puede configurarse TKIP para cambiar claves cada 2 minutos o menos, lo que puede afectar al rendimiento.
- Septiembre 2009, investigadores de la universidad de Hiroshima rompen cifrado WPA en 4 min.

WPA - Personal o WPA - PSK

- Cliente y AP disponen de una clave de acceso prefijada para permitir el acceso de la red inalámbrica (igual que WEP). La PSK inicial es modificada después con TKIP.

WPA - Enterprise

- Cada Cliente autentica su acceso al AP empleando un servidor de autenticación (RADIUS). La gestión de la autenticación se realiza empleando el estándar IEEE 802.1x, cuya base es el protocolo EAP (Extensible Authentication Protocol).
- EAP se emplea en otros entornos, como VPNs, y permite realizar la autenticación de un cliente contra un servidor de autenticación.
- El potencial de EAP es que permite múltiples mecanismos de autenticación (CHAP, Kerberos, certificado de seguridad, autenticación con clave pública, etc.)

EAP/TLS: Basada en un certificado de servidor y cliente.

EAP/TTLS o PEAP: Basada en un certificado de servidor. El cliente se valida con un nombre de usuario y contraseña en un servidor RADIUS. (Por ejemplo el wifi de la UA).

LEAP (Lightweight EAP): Propiedad 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, uno de los cuales es CHAP, que permite el intercambio de la contraseña del usuario cifrada.

- El objetivo de estos mecanismos es proporcionar a un usuario autorizado la MK (Master Key), clave primaria con la que se inicia el mecanismo de cifrado TKIP.

IEEE 802.11i - WPA2™

RSNA - Robust Security Network Association: Proporciona un sistema con integridad y confidencialidad.

- No se introducen variaciones en los mecanismos de autenticación empleados en WPA (WPA2-Personal y WPA2-Enterprise), pero sí permite mejorar la seguridad del cifrado, ya que permite emplear, además de TKIP, otro mecanismo de cifrado denominado AES (Advanced Encryption Standard).
- AES es un standard de cifrado del NIST (Instituto Nacional de Estándares de EE.UU) adoptado como mecanismo estandar de cifrado por el gobierno de EE.UU.
- AES emplea claves de cifrado de 128 bits cuando se emplea en WPA2. En la actualidad, este esquema de cifrado no se ha roto y por tanto es el más recomendable para accesos Wi-Fi.

Tema 5 Diapositivas: Nivel de Red

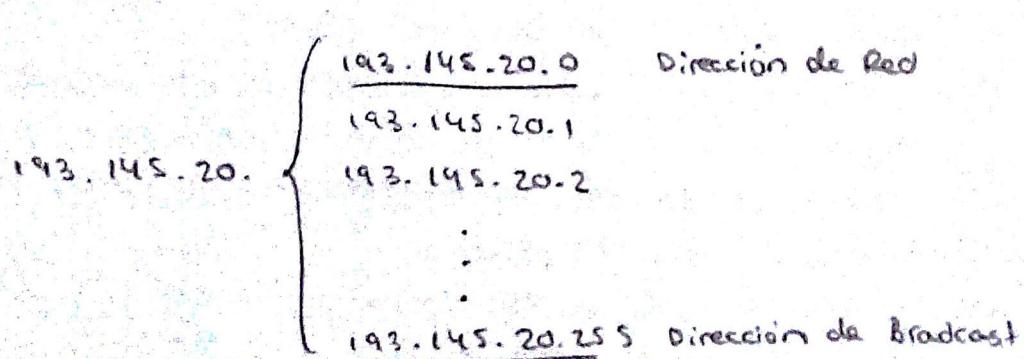
Protocolo IP, RFC 791

- Sistema de numeración para identificar máquinas en una red formada por la interconexión de diferentes segmentos físicos.
- Define un formato de paquete de red (internet) para el control del encaminamiento

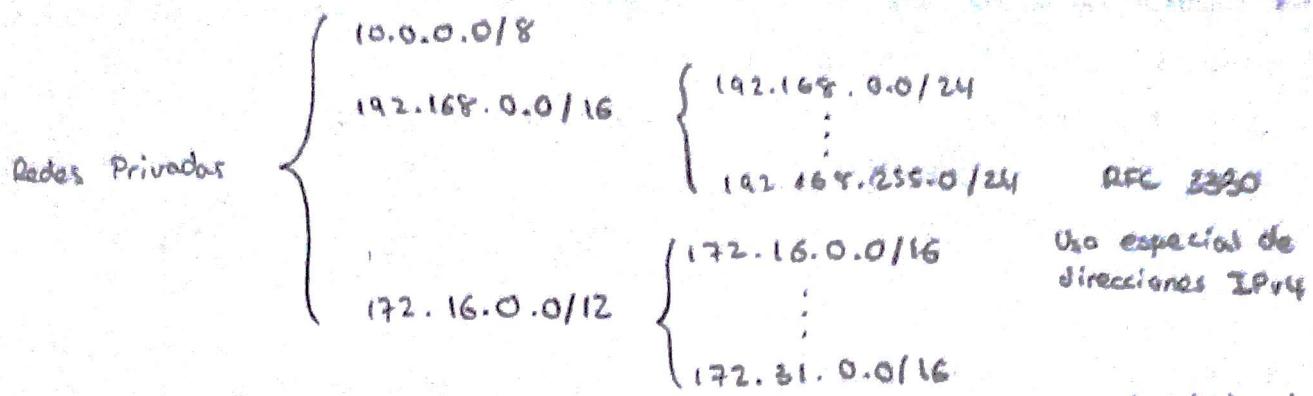
0	15 16	31
Versión 4 bits	HL 4-bit	TOS 8-bit
Identificación	Flag 8 bit	Fragment offset 13 bit
TTL 8 bit	Protocolo 8 bit	Suma Control Cabecera 16 bit
Dirección IP Fuente 32 bit		
Dirección IP Destino 32 bit		
Opciones (si existen) Múltiplo de 32 bit		
Datos		

CLASES

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



Las direcciones de red y broadcast son direcciones reservadas



- Todas las estaciones de una red de difusión que comparten un medio físico 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, siendo, en general, suficiente con redes de clase C (hasta 254 máquinas).
- En las redes punto a punto, las estaciones en los extremos de una red tienen que tener asignada la misma dirección de red IP y en cada enlace punto a punto se especifica una dirección de red IP. Esto desemboca en el desaprovechamiento de las direcciones 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: 2 para máquinas, 1 para red y 1 para difusión.

Formato de tabla de rutas o tabla de encaminamiento

- Tiene una fila (cabecera) por cada red IP que conoce el router.
- 3 tipos de entrada
 - Asociadas a redes conectadas directamente (la puerta de enlace es una IP del router).
 - Asociadas a redes alcanzables (la puerta de enlace es la IP de un router).
 - Puerta de enlace por defecto (la puerta de enlace es la IP de un router).

Destino	Máscara de red	Puerta de enlace
10.1.10.0	255.255.255.0	10.1.10.1
10.2.10.0	255.255.255.0	10.1.10.3
0.0.0.0	0.0.0.0	10.1.10.4

- Para reducir el tamaño de las tablas, cuando hay muchas redes por una misma puerta de enlace la dirección de destino y la máscara de red serán la 0.0.0.0, es decir cuando una red no está en la tabla se envíe a la 0.0.0.0

Sistemas Autónomos (SA)

Sistema Autónomo: 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.

- El encaminamiento óptimo en Internet requiere del intercambio de información de encaminamiento entre todos los routers de Internet, lo cual es impracticable.
- Como solución se ha propuesto un intercambio de información a dos niveles
 - Intercambio de información de encaminamiento entre sistemas autónomos (BGP - Border Gateway Protocol)
 - Intercambio de información de encaminamiento dentro de sistemas autónomos (RIP- Routing Information Protocol, OSPF- Open Shortest Path First).

BGP (Border Gateway Protocol)

- En cada SA se especifica un router de frontera (generalmente uno aunque pueden ser más) que dialoga con los routers de frontera de otros sistemas autónomos.
- La info de encaminamiento se intercambia mediante TCP (puerto 179) entre routers frontera.
- BGP informa acerca de alcanzabilidad y conectividad entre sistemas autónomos (que redes pertenecen a qué SAs), además reduce la info intercambiada comunicando una sola vez a todos las redes accesibles a través de un SA, y después actualiza la info que se modifica. Agrupa destinos en una sola denominación.
- BGP soporta autenticación para preservar la validez de la info de encaminamiento intercambiada.

BGP Open: El primer mensaje intercambiado entre routers frontera que establecen la conexión. Se intercambian parámetros como el identificador de SA, intervalos de tiempo en el envío de mensajes BGP, etc..

BGP Update: Informa acerca de destinos existentes en el SA y destinos que se han eliminado en el SA.

BGP Keepalive: Informa que un extremo de la comunicación sigue activo. TCP no controla que los 2 extremos estén activos cuando no intercambian datos, por lo que BGP define un mensaje para este propósito.

BGP Notification: Informa acerca de errores en la comunicación BGP (mensajes BGP con errores: rutas incorrectas o incongruentes) y permite el control en la comunicación (finalización de conexión, expiración de tiempo de espera de mensajes keepalive.)

Cabecera				Datos		Mensaje BGP
Marcador	Longitud	Tipo	Datos			
16 bytes	2 bytes	1 byte	Longitud Variable			

- Para poder conseguir conectividad en Internet todos los SA tienen que estar conectados al backbone de Internet para intercambiar BGP pero como no cualquier ISP puede estar conectado al backbone de Internet (ARPANET - NSFNET en USA), existen los Network Access Point (NAPs).
- En cada NAP acceden los SA de varios ISPs que intercambian información de encaminamiento con BGP entre el backbone de Internet y los ISPs.
- Para evitar inconsistencias en el encaminamiento entre ISP, en cada NAP hay un router servidor (RS) con el que dialogan los routers frontera de los ISPs para el intercambio de BGP.

ISP (Internet Service Provider): Proveedor de acceso a internet.

Protocolo de Información de Encaminamiento (RIP)

- Se fundamenta en un algoritmo de vector de distancia (Bellman-Ford).
- Cada router dispone de una tabla con info de destinos y una métrica (nº 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 mas cortas a un mismo destino.
- Existe un número máximo de saltos para la métrica de RIP, que es 16. Esto evita problemas de convergencia del algoritmo, es decir, llegar a una solución estable.
- Los mensajes RIP se envían dentro de paquetes UDP, y para que lleguen a todas las estaciones del segmento físico (difusión), los paquetes UDP se envían a la dirección de Broadcast de la red IP donde se difunden.
- RIP presenta problemas de convergencia lenta ante cambios en la red y posibilidad de que se introduzcan bucles infinitos. Para evitar esto emplea estrategias como temporizadores y número máximo de saltos

OSPF - Open Shortest Path First

- Se basa en el algoritmo Dijkstra sobre un grafo que representa la red y del cual cada nodo son routers.
- Los caminos tienen un peso o coste asignado considerando las características del enlace (alta/baja velocidad, activado/desactivado, etc...)

OSPF Hello: Determina qué vecinos tiene accesible un router

OSPF Database description: Informa de la topología de la red de comunicaciones.

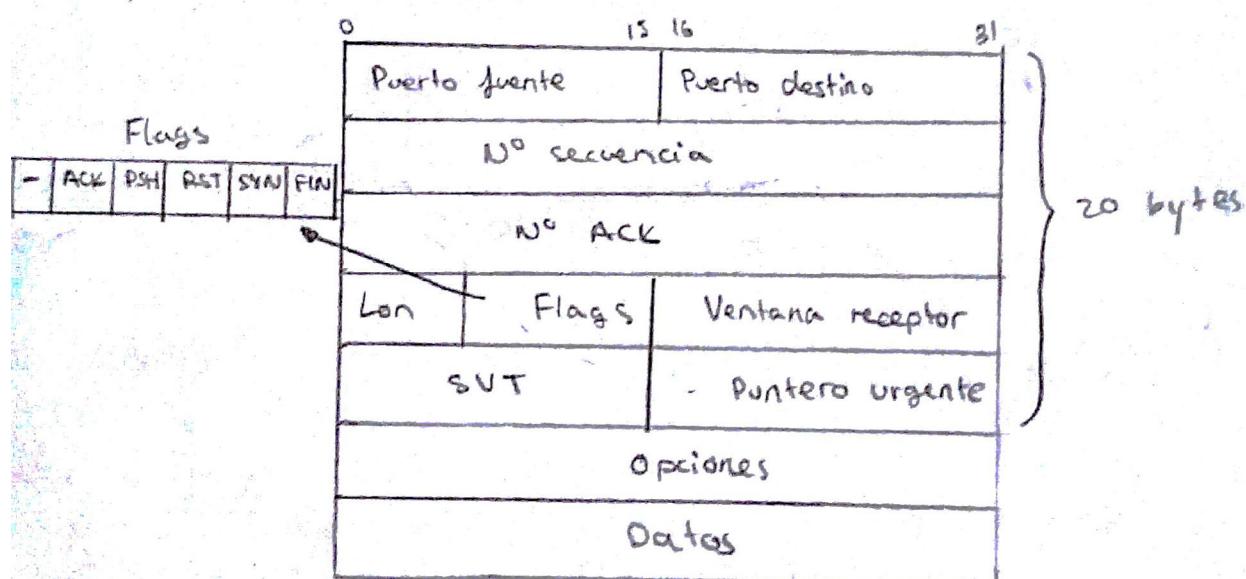
OSPF Link status request: Solicita a los routers vecinos información sobre los enlaces activos.

OSPF Link status update: Un router informa a sus vecinos del estado de sus enlaces.

- Los mensajes OSPF se encapsulan en paquetes IP enviados a la dirección de multicast 224.0.0.5 y 224.0.0.6.
(todos routers OSPF / routers OSPF designados)

Protocolo de Control de la Transmisión (TCP)

- Trabaja con un flujo de bytes, que TCP agrupa en paquetes de tamaño adecuado para mejorar el rendimiento y evitar a la vez la fragmentación a nivel IP.
- Transmisión orientada a conexión. Se requiere una secuencia de conexión previa al envío - recepción de datos entre cliente y servidor, y una desconexión total.
- Es fiable, ya que emplea control de flujo mediante ventana deslizante de envío continua y asentamientos positivos o ACK's para confirmar las tramas válidas recibidas. La ventana deslizante se aplica a los bytes: se numeran y confirman bytes y no paquetes.
- Flujo de bytes ordenado. Aunque IP trabaja con datagramas, un receptor TCP ordena los paquetes que recibe para entregar los bytes al nivel superior en orden.



Nº secuencia: Número de secuencia de numeración del primer byte del campo de datos del paquete.

Nº ACK: Número de la siguiente secuencia de numeración de los bytes del campo de datos que se espera recibir.

Flags: Campo con bits con significado propio.

ACK: Si es 1 el ACK es válido y debe interpretarse, es decir, el paquete es un ACK.

PSH (push): Si es 1 indica que la capa de transporte debe pasar los datos a la capa de aplicación sin esperar a recibir más datos.

RST (reset): Indica un rechazo de la conexión.

SYN (synchronize): Se utiliza para solicitar establecimiento de una conexión.

FIN: Se utiliza para solicitar la liberación de una conexión.

Ventana: Sirve para informar sobre el número de bytes que el emisor del paquete es capaz de recibir en su buffer de recepción. Si vale 0 indica que no puede recibir datos, aunque si interpretar paquetes con flags.

MSS

- El MSS (Maximum Segment Size) es la cantidad máxima de datos que puede incorporar un paquete TCP. Este valor depende del MTU de la red donde se transmite el paquete TCP.
- Para evitar la fragmentación, el establecimiento de la conexión se negocia con el valor del MSS.

Cálculo del tiempo de espera de ACK. Algoritmo de Karn

- El tiempo de espera de un ACK (timeout) se calcula dinámicamente durante el funcionamiento de TCP a partir del RTT (Round Trip Time) o tiempo de ida y vuelta, el cual se calcula como el tiempo transcurrido desde el envío de un segmento y la llegada de su ACK.

$$\boxed{\text{Timeout} = \beta \cdot \text{RTT}}$$

donde β está establecido entre 1 y 2, de forma que se consiga un reenvío adecuado.
(se recomienda 2)

- El algoritmo de Karn redefine la fórmula anterior para evitar errores de retraso elevado de ACK y lo hace del siguiente modo.

$$\boxed{\text{nuevo Timeout} = \gamma \cdot \text{Timeout}}$$

donde γ toma el valor 2