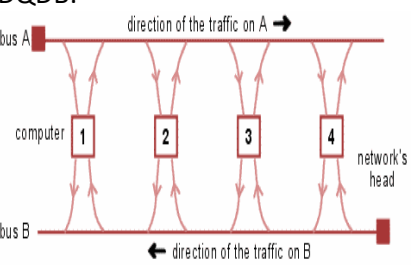


- Modelo OSI (Open Systems Communication):
- ATM (Asynchronous transfer mode): Red de 1990 que transfiere millones de bits por segundo (1Mbps)
- Modelo TCP / IP (Transmission Control Protocol / Internet Protocol ): Describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.
- Redes de Difusión: Las redes de difusión son aquéllas en las que la señal emitida por un transmisor es recibida por cualquier terminal conectado a la red. Se realiza indicando un código especial en el campo de dirección del mensaje para que todas las máquinas puedan procesarlo.
- Red de Multidifusión: La señal emitida por un transmisor es recibida por cualquier un conjunto determinado y concreto de hosts conectados a la red. Ej. De 5 ordenadores solo 3. Se reserva un bit del campo dirección en el mensaje para indicar multidifusión siendo los n-1 bits restantes del campo de dirección empleados para direccionar grupos de máquinas en la red
- Red Punto a Punto: Se establecen múltiples conexiones entre pares individuales de máquinas. Para realizar la transmisión es posible que el mensaje deba visitar máquinas intermedias. Como existen rutas alternativas para la comunicación de dos hosts el fallo medio de transmisión es menos. Por el contrario, son más caras que las de difusión.

Características	LAN	MAN	WAN
Acrónimo	Local Area Network	Metropolitan Area Network	Wide Area Network
Coste	La más barata	Más cara que LAN	La más cara
Velocidad (Mbps)	10 - 10 (Gbps)	10 – 100	57 (Kbps) – 20
Rango (Km)	1	50	10 000
Topología	Bus común y anillo	Bus Dual de Cola Distribuida (DQDB)	Estrella, anillo, árbol, malla, irregular...
Ubicación de los ordenadores conectados a la red	En el mismo edificio	En la misma ciudad usando módems o líneas de teléfono	Distribuidos por el país o por el continente. Conexión vía satélite o Internet (Conexiones punto a punto)
Ejemplos / Más datos que no me importan pero que deberías saber por si cae en el examen	Una oficina con diferentes departamentos conectados a una red. Bus común Ethernet (IEEE 802.3) Topología anillo Token Ring (IEEE 802.5)	Un banco cuyas sucursales están distribuidas por la ciudad. DQDB: 	Las oficinas alrededor del mundo de Google. 2 tipos: -Públicas: Moderador es una entidad pública o está abierta a un público general. Ej. RTC – Red Telefónica Conmutada RDSI – Red Digital de Servicios Integrados  -Privadas: Moderador es una entidad corporativa y la emplea para fines propios. SNA o DNA por ejemplo

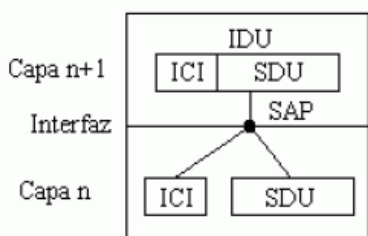
Las redes WAN también se pueden clasificar por la forma de establecer la comunicación en la red:

- a) Conmutación de circuitos: Switches físicos
- b) Conmutación de paquetes: Conversión de señal digital a analógica (por el modem)

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

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

- Servicios: Conjunto de funciones (primitivas de servicio) que una capa ofrece a su capa adyacente superior (comunicación vertical).



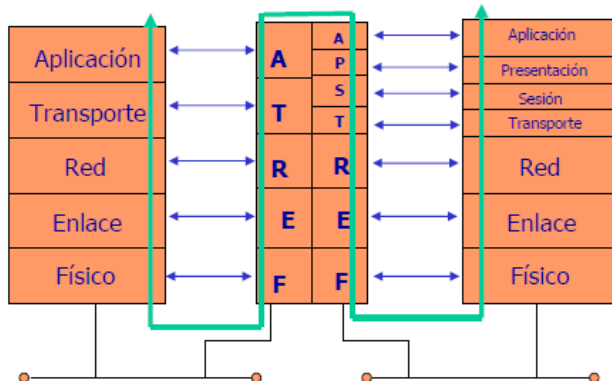
SAP: Punto de acceso al servicio

IDU: Unidad de datos de la interfaz

ICI: Información de control de la interfaz

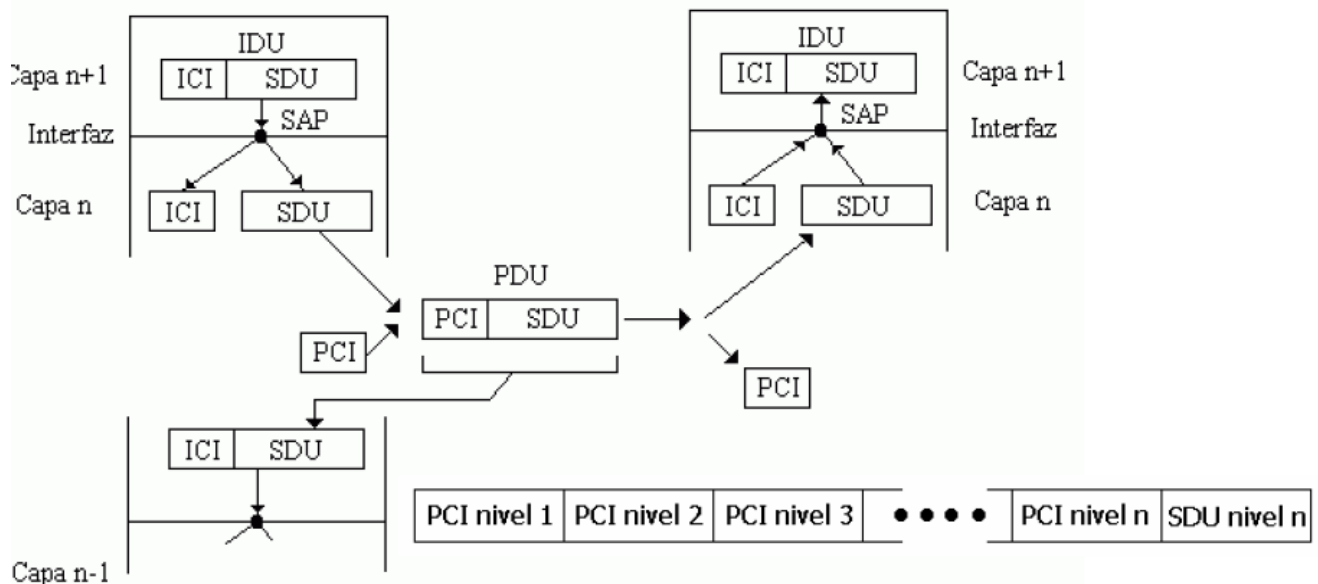
SDU: Unidad de datos del servicio

### Interconexión de redes a nivel de aplicación. Pasarela (Gateway)



- Protocolo: Conjunto de reglas de utilización de las primitivas de servicio suministradas por el nivel inferior para la comunicación a nivel horizontal
- Comunicación horizontal y vertical en el modelo OSI:

## Comunicación horizontal y vertical en el modelo OSI



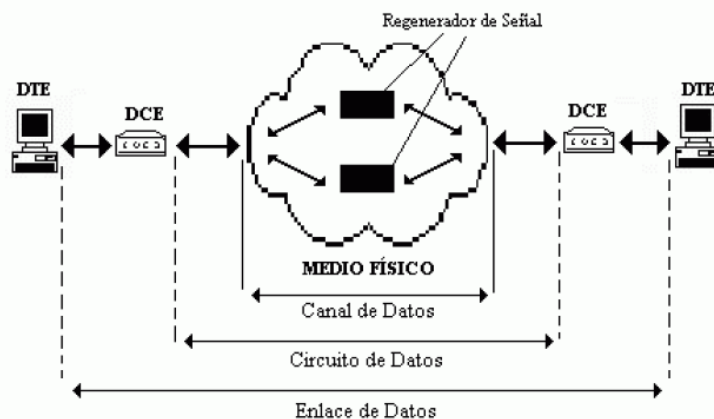
**PDU: Unidad de datos del protocolo**

**PCI: Información de control del protocolo**

- Protocolo de nivel n: Conjunto de normas para el intercambio de PDU (Protocol Data Unit) entre entidades pares de nivel n (comunicación horizontal).
- Fragmentación en el protocolo de la capa n: Mecanismo para incorporar en una PDU (Unidad de datos del protocolo) de tamaño limitado una SDU (Unidad de Datos del Servicio). La fragmentación es necesaria para que los errores provoquen reenvíos de PDUs limitadas en tamaño.

• Tema 3

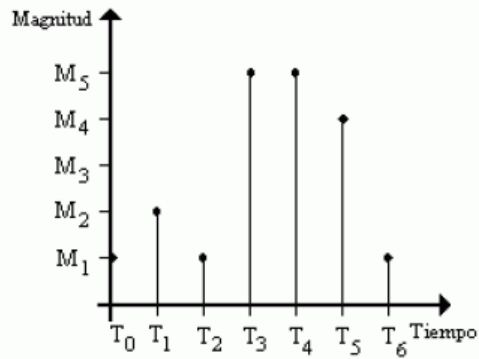
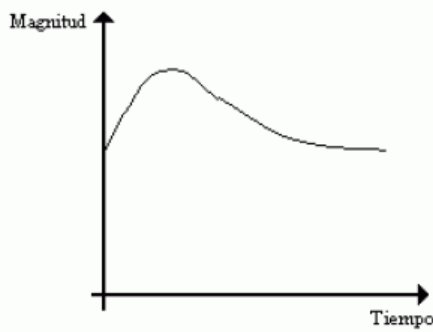
- DTE: (Data Terminal Equipment) Equipo Terminal de Datos.



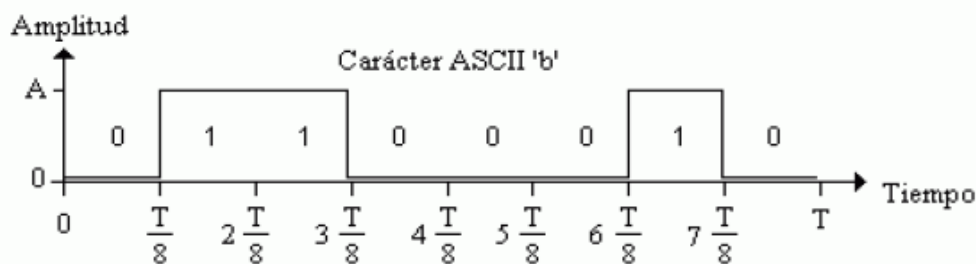
- DCE: (Data Circuit-Terminating Equipment) Equipo Terminador de Circuito de Datos.

## Señal analógica

## Señal digital



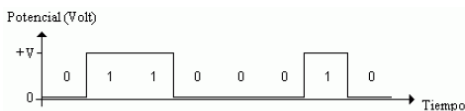
- Señal analógica y periódica de pulsos asociada a la transmisión secuencial de un carácter ASCII



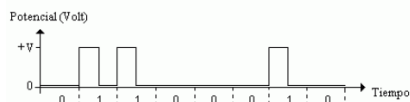
- Codificación binaria: Cada valor lógico de la señal de información tiene asignado un nivel de tensión eléctrica (valor de la magnitud física).

Sin retorno a 0

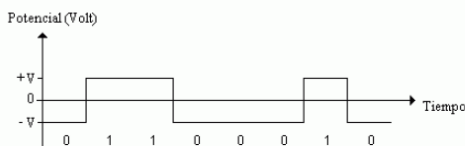
Con retorno a 0



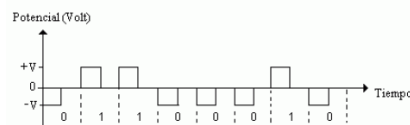
UNIPOLAR



UNIPOLAR

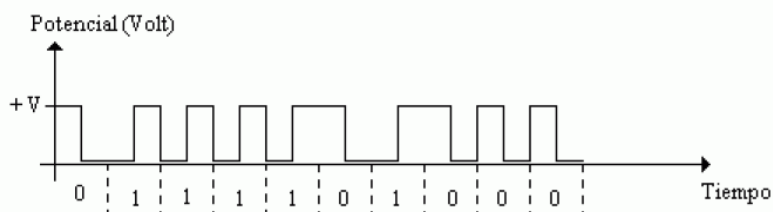


BIPOLAR



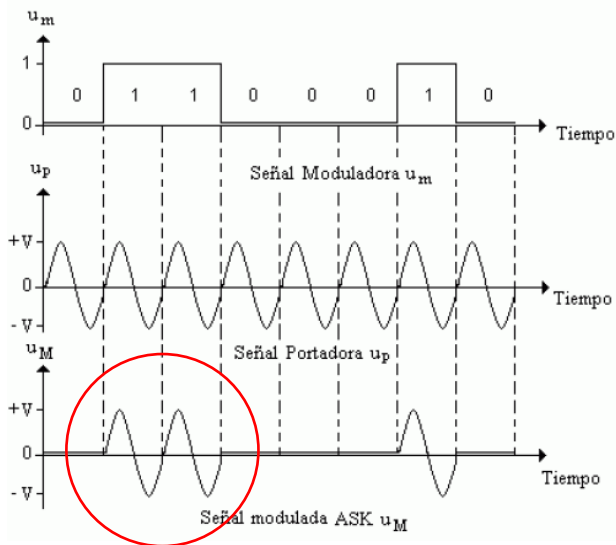
BIPOLAR

- Codificación Manchester: Cada valor lógico de la señal de información tiene asignado un tipo de transición en el cambio del valor de la tensión eléctrica (valor de la magnitud física).

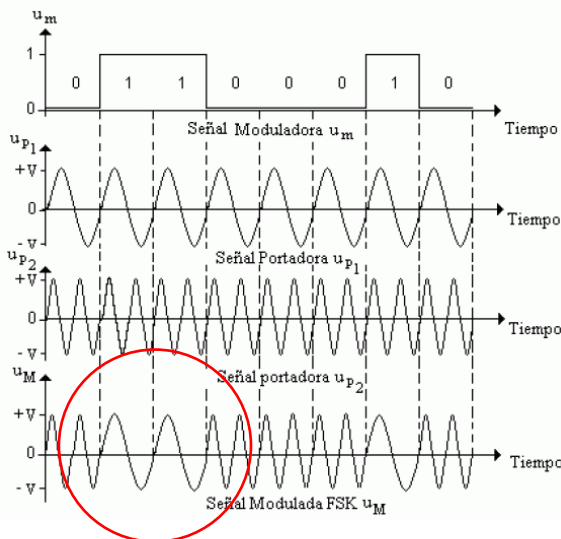


- Señal moduladora: señal de información a transmitir.
- Señal portadora: señal con unas características que permite su transmisión por el medio físico.
- Señal modulada: señal portadora transmitida en el medio modificada en función de las características de la señal moduladora.

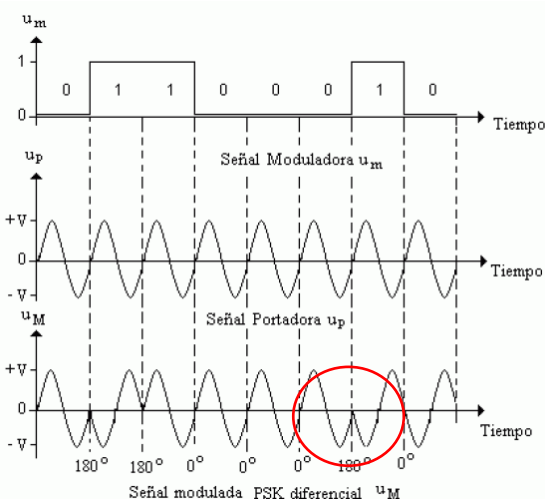
- Señal moduladora: DIGITAL (Señal de pulsos con información binaria)
- Señal portadora: ANALÓGICA (Señales periódicas senoidales)
- Modulación por cambio en amplitud (ASK - Amplitude shift keying): La señal se modula cuando el valor de la señal moduladora es 1. De lo contrario (si fuera 0) se mantiene estable y constante



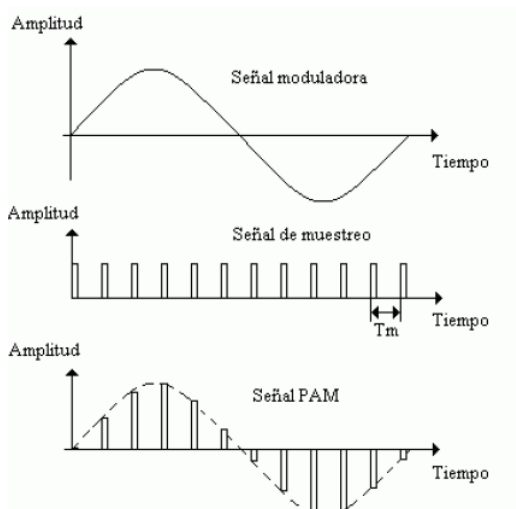
- Modulación por cambio en frecuencia (FSK - Frequency shift keying): La señal se modula (cambia de frecuencia) cuando el valor de la señal moduladora cambia de 0 a 1 o de 1 a 0



Modulación por cambio en fase (PSK - Phase shift keying): La señal se modula (repite de frecuencia) cuando el valor de la señal moduladora cambia de 0 a 1 o de 1 a 0



- Modulación digital
- Señal moduladora: ANALÓGICA (Señales periódicas senoidales)
- Señal portadora: DIGITAL (Señal de pulsos)
- Modulación por código de pulsos (PCM - Pulse code modulation): La señal se modula de una señal analógica en una secuencia de bits (señal digital). Los niveles de cuantificación digital son linealmente uniformes.



$$f_m = 2B_{señal}$$

Señal PAM - Señal Pulso Analógico Modulada

- Medios de transmisión:

Nombre	Cable par paralelo	Cable par trenzado no blindado (UTP)	Cable coaxial	Fibra óptica	Ondas electromagnéticas
Imágen		 			
Distancia máx	50 m	Categoría 3 - 100 m Categoría 5 - 100 m Categoría 6 - 100 m	100 m	Dispositivo regenerador de señal en el punto de corte.	
Velocidad	20 Kbps	Categoría 3 - 30 Mbps Categoría 5 - 100 Mbps Categoría 6 - 1000 Mbps	1000 Mbps	<b>Multimodo</b> 20 MHz/Km <b>Índice gradual</b> 500 - 1000 MHz/Km <b>Monomodo</b> 1 - 10 GHz/Km	2.4 y 5 GHz. 600 Mbps.
Características	Comunicaciones DTE - DCE	Reduce el ruido cruzado o diafonía	La malla conductora evita las interferencias de campos eléctricos externos al cable, elimina el ruido de impulso. <b>Cable coaxial 50 W</b> Transmisión en banda base (Manchester).	Núcleo de cristal de sílice rodeado de un recubrimiento de silicona. Dispone de una capa externa como protección hecha de poliuretano. Medio que permite el confinamiento y propagación	La radiación electromagnética es un mecanismo de transmisión de energía que presenta las propiedades de una onda. Esta onda es susceptible de incorporar información empleando mecanismos de

			<p>Redes LAN (sustituido por pares trenzados). Velocidad de 10 Mbps a distancia de 100 m. para cable coaxial fino. Velocidad de 10 Mbps a distancia de 500 m. Para cable coaxial grueso.</p> <p><b>Cable coaxial 75 W</b></p> <p>Transmisión en banda modulada. Multiplexión en frecuencia de múltiples canales (transmisión broadband - 300 MHz). Televisión analógica/digital por cable.</p>	<p>de un haz de luz. La propagación de la luz entre dos medios distintos distorsiona la trayectoria del haz, produciéndose una refracción o reflexión.</p> <p>A) Fibra multimodo o de índice de salto. Existen múltiples haces que se propagan en la fibra, desfasándose temporalmente debido a los diferentes recorridos ópticos</p> <p>B) Fibra de índice gradual. El índice de refracción variable en el núcleo permite compensar el efecto de la dispersión intermodal.</p> <p>C) Fibra monomodo. Un núcleo de diámetro muy reducido (<math>&lt; 10 \mu\text{m}</math>) permite la propagación de un único haz en paralelo al eje de la fibra. No existe dispersión intermodal, pero si dispersión intramodal.</p>	<p>modulación (ASK, PSK, FSK).</p> <p>El espectro de radiocomunicación es el conjunto de frecuencias de radiación electromagnética que se han definido para incorporar información y se emplean en los sistemas de comunicaciones. Esta elección es por diversos motivos salud, energético...</p>
--	--	--	--	--	---

- Nivel de enlace: Función genérica: Comunicación libre de errores en un medio físico.
- Funciones:
  - Delimitación de tramas: Identificación del inicio y fin de un paquete
  - Direccionamiento: Identificación de los extremos de la comunicación en un medio físico
  - Control de errores: Asegura una transmisión sin errores debidos al medio físico
  - Control del flujo: Control del flujo de tramas entre emisor y receptor para evitar saturaciones, reenvíos incorrectos, etc.
- Formato:

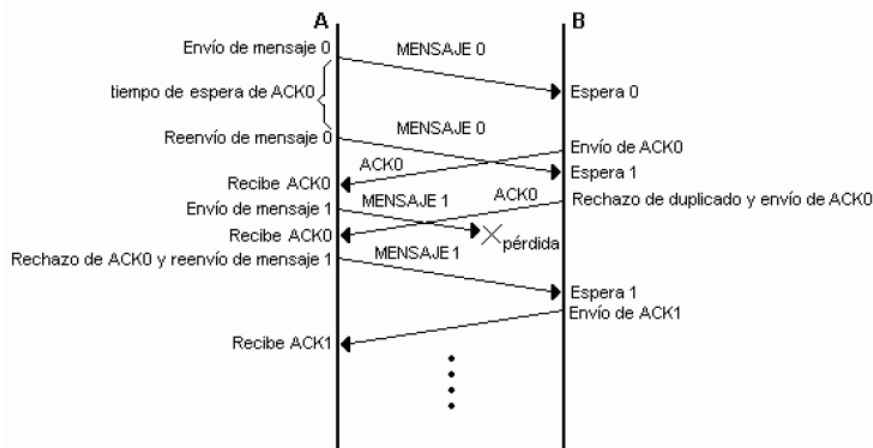


Formato de la trama Ethernet

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

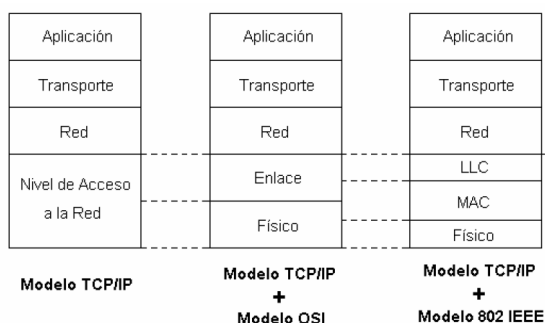
- Direccionamiento: El objetivo es identificar los elementos que intercambian tramas de nivel de enlace en un medio físico. Para ello, se asignan secuencias de bits únicas a cada estación.
  - Implícito: No es necesario especificar las estaciones origen y destino que intercambian tramas. Ej: línea punto a punto.
  - Explícito: Es necesario especificar las estaciones origen y destino que intercambian tramas. Ej: Ethernet.
- Control de Errores:
  - Secuencia de Verificación de Trama (Frame Check Sequence (FCS)): Conjunto reducido de datos que suele añadirse en la cola de un paquete de enlace. Dependiendo del tipo de información en la FCS se distingue entre: A) Códigos de detección de error B) Códigos de corrección de error. En A) solo permite detectar si el paquete tiene algún bit erróneo, en B) el receptor puede identificar el problema y corregirlo. Este método no se emplea actualmente.
  - Detección de errores por paridad de bits de datos: Permiten detectar si en el paquete hay errores en un número impar de bits. Incorporan mucha información redundante, en comparación con otros sistemas.
  - Detección de errores por Códigos de Redundancia Cíclica (CRC): Asocia un bloque de datos a un polinomio en x, determinando la SVT mediante operaciones y propiedades de polinomios. La elección del polinomio generador se realiza para cumplir con las propiedades de detección de errores más adecuadas
- Algoritmos de control de flujo (↔):
  - Controlar el envío y recepción correcto de los paquetes de nivel enlace
  - Controlar la sincronización del emisor y receptor de datos
  - Evitar congestiones en el envío de información del emisor al receptor
- Protocolos de parada y espera: El control del flujo se establece en que el emisor debe esperar a una confirmación por parte del receptor por cada bloque de datos enviado para poder continuar la transmisión. Presenta 2 problemas, duplicación y pérdida de la sincronización. Solución:
  - Duplicación -> Numeración de las tramas con un bit ( 0 - 1 - 0 - 1 - 0 ...)
  - Pérdida de la sincronización - > Numeración de los ACK con un solo bit ( 0 - 1 - 0 - 1 - 0 ...)





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

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



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

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

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

### IEEE 802.3: Ethernet (CSMA/CD)

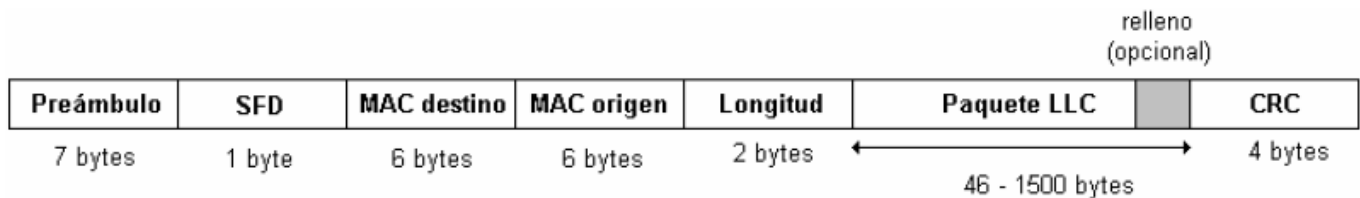
### IEEE 802.5: Token Ring (Anillo con testigo)

## IEEE 802.11x: LAN Inalámbrica

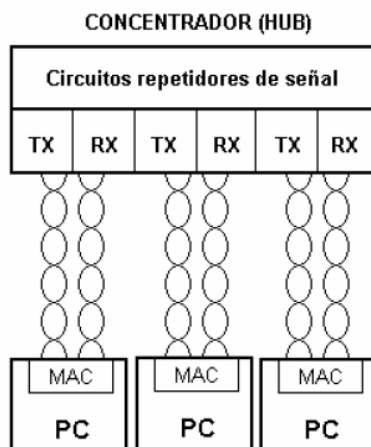
### IEEE 802.1Q: LAN Virtual (VLAN)

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

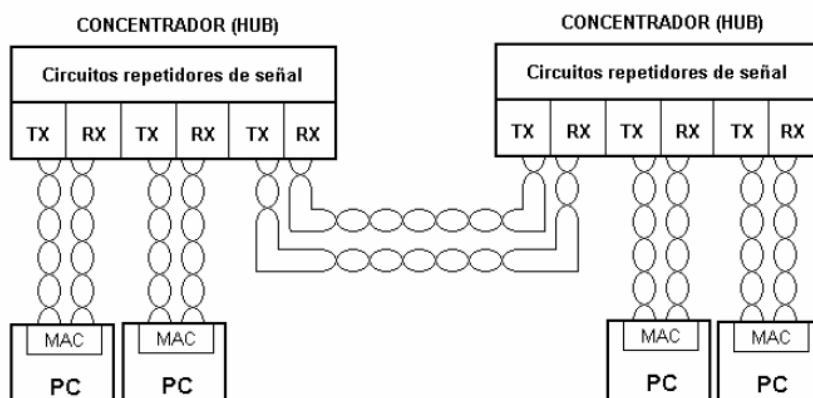
- Ethernet: Una red Ethernet se caracteriza por emplear un medio físico compartido (cable coaxial, cable par trenzado o fibra óptica) entre todas las estaciones con topología de bus. Semiduplex y emplean un mecanismo denominado CSMA/CD (bus) para el reparto del medio físico.
- IEEE 802.3: Establece un formato de paquete donde se especifica la cabecera MAC:
  - Preámbulo: Secuencia de 7 bytes
  - SFD: Delimitador de inicio de trama
  - MAC destino/origen: Identificador de 48 bits para cada equipo
  - Longitud: Tamaño del campo de datos del paquete (máximo 1500)
  - CRC: Código de Redundancia Cíclica de 32 bits para detección de errores



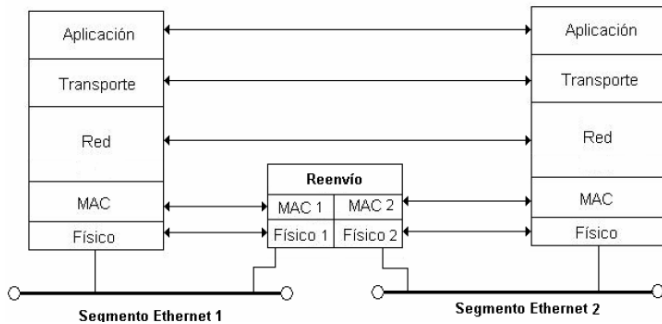
- CSMA/CD: Comprueba el medio físico antes de transmitir un paquete de datos. El esquema de funcionamiento de CSMA/CD siempre es semiduplex.
  - Problemas: Colisión por comprobación simultánea del bus por dos o más estaciones
  - Solución: En cada intento se espera un número aleatorio de veces antes de volver a intentar emitir una señal
- Concentrador Ethernet (Hub): Topología en estrella. Las colisiones se detectan cuando se recibe una señal por el par de recepción al mismo tiempo que se transmite una trama.



- Repetidores (hubs en cascada): La conexión de concentradores en cascada permite el aumento en el tamaño físico de la red Ethernet.



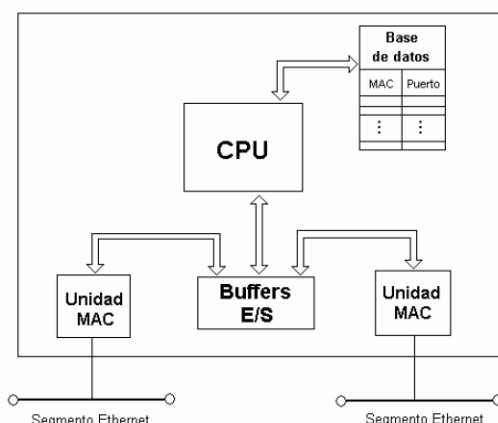
- **Bridges:** Un brige es un dispositivo de interconexión entre dos o más segmentos Ethernet que analiza la cabecera MAC de los paquetes para determinar si hay que reenviarlos o no de un segmento a otro.



- Los puentes denominados puentes transparentes son aquellos en los que la decisión de cómo los paquetes se intercambian entre segmentos la toman ellos (los equipos no conocen la estructura de la red). Modo de funcionamiento:
  - En el modo de reenvío se comprueba la dirección MAC de destino de cada paquete Ethernet que llega a un puerto.
  - Si la dirección MAC de destino se encuentra en la tabla de reenvío, el puente reenvía el paquete al puerto asociado (siempre que el puerto asociado sea distinto del puerto por donde ha llegado el paquete)
  - Si la dirección MAC de destino no existe en la tabla de reenvío, el paquete se reenvía a todos los puertos excepto por el que se recibió.
  - Los paquetes con dirección de destino la dirección de broadcast se reenvían a todos los puertos, excepto al puerto por el que se recibió el paquete de difusión.

Modo de aprendizaje:

- En el modo de aprendizaje se comprueba la dirección MAC de origen en cada paquete Ethernet recibido en un puerto.
- Si la dirección MAC de origen no se encuentra en la tabla de reenvío, el puente crea una entrada con la dirección MAC de origen y el puerto donde se ha recibido.
- Cada entrada en la tabla de reenvío de un puente tiene asociado un temporizador (segundos) que mide el tiempo desde que se creó la entrada en la tabla.
- Si se recibe un paquete con una dirección MAC de origen por el puerto que se indica en la tabla de reenvío, el temporizador se inicializa a cero.



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

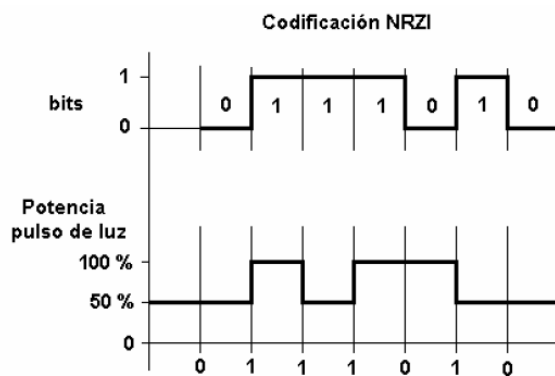
**Buffers E/S:** Unidad de almacenamiento de tramas en proceso (lectura/envío). FIFO.

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

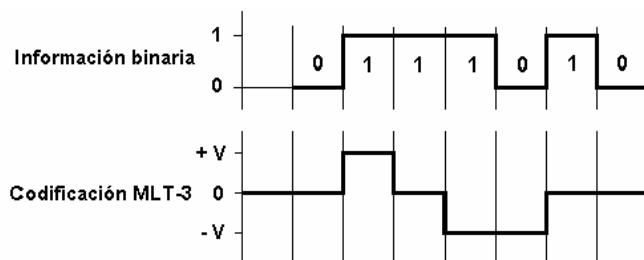
Modo de aprendizaje: mediante el algoritmo Spanning Tree.

- **Ethernet Conmutada:** cada puerto se conecta un equipo en vez de un segmento de red. Estos dispositivos se denominan conmutadores o switches. Existe Ethernet mixta de concentradores/conmutadores
- **Fast Ethernet (IEEE 802.3u):** redes Fast Ethernet funcionan con conmutadores, permitiendo el modo de trabajo half-duplex (CSMA/CD) y full-duplex. El conmutador debe emplear los buffers del puerto del servidor para repartir el tráfico de los clientes, es decir repartir el ancho de banda de 10 Mbps entre los clientes.

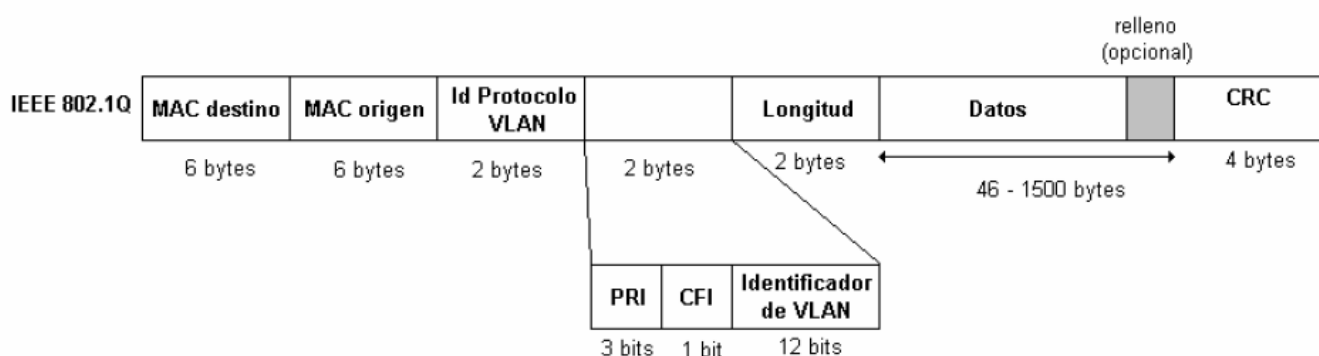
- 100BaseX (IEEE 802.3u): El principal problema de la transmisión a alta velocidad es la sincronización emisor-receptor al transmitir la secuencia de bits. Para introducir siempre información de sincronización en el flujo de bits, 100BaseX introduce una codificación 4B/5B. Cada símbolo de 5 bits se convierte en pulsos luminosos empleando codificación NRZI



- 100BaseTX (IEEE 802.3u): 100BaseTX emplea la normativa 100BaseX de codificación 4B/5B sobre cable UTP categoría 5 (máximo 100 metros). Cada símbolo de 5 bits se convierte en pulsos eléctricos empleando la codificación MLT-3.

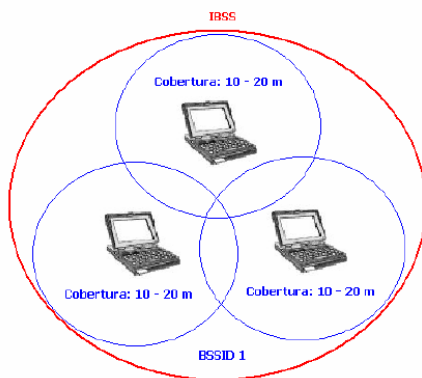


- Gigabit Ethernet (IEEE 802.3z): Las redes Gigabit Ethernet funcionan con conmutadores, permitiendo el modo de trabajo half-duplex (CSMA/CD) y full-duplex.
- 1000BaseT (IEEE 802.3z): 1000BaseT permite alcanzar 1 Gbps a distancias de 100 metros empleando los cuatro pares de hilos para transmitir y recibir simultáneamente (cancelación de eco).
- 1000BaseX (IEEE 802.3z): La transmisión de datos a 1 Gbps por fibra óptica es menos compleja debido al enorme ancho de banda de la fibra. Los bits del paquete Ethernet son modificados con un codificador 8B/10B, introduciendo información de sincronización para el receptor.
- 10 Gigabit Ethernet (802.3ae): Las redes 10 Gigabit Ethernet (10GBase-XX) funcionan con conmutadores permitiendo solamente el modo de trabajo full-duplex (no existe el CSMA/CD). Emplea en general la fibra óptica como medio de transmisión
- 2.5GBaseT – 5GBaseT (802.3bz): Esta normativas están pensadas para ser empleadas con cable par trenzado (UTP) de categoría 5e (2.5 Gbps) y categoría 6 (5 Gbps) y distancias hasta 100 metros. Su objetivo es permitir conexiones de puntos de acceso Wi-Fi de la norma 802.11ac.
- IEEE 802.1Q. Redes de Área Local Virtuales (VLAN): Cada dominio de difusión independiente. El funcionamiento de un conmutador VLAN es similar al de un puente, disponiendo de una tabla de reenvío (Cada VLAN tiene asociada una dirección de red IP diferente para que ARP funcione).



- El formato de trama IEEE 802.1Q se emplea cuando se interconectan conmutadores VLAN entre sí, o un router a un conmutador VLAN. Un conmutador VLAN maneja de diferente forma los enlaces de acceso y los enlaces troncales:
  - En los enlaces de acceso los paquetes tienen el formato del IEEE 802.3.
  - En los enlaces troncales los paquetes tienen el formato del IEEE 802.1Q. Los conmutadores VLAN emplean un protocolo denominado GVRP (GARP VLAN Registration Protocol).
- IEEE 802.11x. LAN Inalámbrica: Una red LAN inalámbrica es una red de área local que emplea ondas electromagnéticas como soporte físico para la comunicación de datos.
- BSS (Basic Service Set): Conjunto de servicio básico. Grupo de estaciones que se comunican entre ellas.
- SSID (Service Set Identifier): Identificador de un BSS. Cadena de 32 caracteres máximo.
- BSSID (Basic Service Set Identifier): SSID en redes ad-hoc.
- ESSID (Extended Service Set Identifier): SSID en redes de infraestructura.

#### Red Inalámbrica ad-hoc



- IEEE 802.11b: Comunicación inalámbrica empleando una señal portadora de 2.4 Ghz. Esta frecuencia está declarada para su uso libre, por lo que pueden existir interferencias con otros dispositivos del mercado.
- IEEE 802.11g: Comunicación inalámbrica empleando una señal portadora de 2.4 Ghz. Con esta normativa se consigue alcanzar velocidades de hasta 54 Mbps.
- IEEE 802.11n: Permite emplear la portadora de 2.4 GHz y la de 5 GHz (19 canales) consiguiendo velocidades de hasta 600 Mbps.
- IEEE 802.11ac: Emplea solamente la portadora de 5 GHz (19 canales) y varias antenas, consiguiendo velocidades de hasta 1.3 Gbps.
- La velocidad de transmisión con wireless no es fija, le afecta el ruido del entorno de trabajo.
- (IEEE 802.11x) La elevada tasa de error en el medio introduce dos necesidades:
  - 1. Tamaño de paquete pequeño. Es necesario un tamaño de paquete más pequeño, pues los errores provocarán reenvíos más pequeños de datos.
  - 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
- El protocolo MAC del 802.11 distingue entre dos modos de funcionamiento para el uso del medio físico:
  - 1. DCF (Función de coordinación distribuida): Empleadas en wireless de infraestructura y ad-hoc.
  - 2. PCF (Función de coordinación centralizada): Empleadas en wireless de infraestructura, donde el AP controla el acceso al medio compartido.
- En el modo DCF cada estación compite por el uso del medio físico. El mecanismo de reparto empleado es el CSMA/CA (Acceso al medio con detección de portadora y evitación de colisiones). Para evitar el problema de la estación oculta (un AP detecta dos estaciones, pero las estaciones no se detectan entre ellas) se introduce un mecanismo de reserva de la red.
- PCF – Función de coordinación centralizada
- Este modo de funcionamiento está definido sólo para las redes de infraestructura, pues precisa de la existencia de un punto de acceso AP.
- Cuando existe un AP todas las comunicaciones se realizan a través de él. Es decir, si una estación quiere transmitir un paquete a otra estación, se enviará la información al AP y éste lo reenviará a la estación

destino.

- Periodo de no colisión: En el periodo de no colisión, el AP envía a una estación un paquete solicitando que le envíe un bloque de datos. Cuando el bloque de datos es recibido por el AP, envía otra solicitud a otra estación.
- Wi-Fi Alliance: Es una asociación de fabricantes de tecnología de red inalámbrica basada en la norma IEEE 802.11x
- Principios de seguridad:
  - Autenticación: Una estación (cliente) debe identificarse como un usuario autorizado de la red Wi-Fi.
  - Integridad de la información: La información debe transmitirse cifrada para evitar espías (sniffers).
- Autenticación y cifrado WEP: WEP (Wired Equivalente Privacy) fue el primer protocolo de encriptación empleado en el estándar IEEE 802.11x. El funcionamiento de WEP está basado en el conocimiento de una misma clave secreta por parte de la estación y el AP (PSK – Pre-Shared Key)
- Autenticación y cifrado WPA: La principal vulnerabilidad de WEP es la capacidad de obtener la clave de cifrado. Así, WPA mantiene el mismo algoritmo de cifrado de WEP (RC4), pero introduce el mecanismo TKIP (Temporal Key Integrity Protocol). TKIP modifica la clave de cifrado entre el cliente y el AP cada cierto tiempo, además de introducir un mecanismo de verificación de la integridad de los paquetes cifrados.
- WPA–Personal o WPA-PSK: En este mecanismo, cliente y AP disponen de una clave de acceso prefijada para permitir el acceso a la red inalámbrica (mismo mecanismo de WEP). La clave PSK inicial es modificada posteriormente en el cifrado al emplear TKIP.
- WPA–Enterprise: En este mecanismo, cada cliente autentica su acceso al AP empleando un servidor de autenticación (RADIUS).
  - EAP/TLS: Autenticación basada en un certificado de servidor y cliente
  - EAP/TTLS o PEAP: Autenticación basada en un certificado de servidor. El cliente se valida con un nombre de usuario y contraseña en un servidor RADIUS
  - LEAP (Lightweight EAP): Autenticación propietaria de Cisco Systems y que no emplea certificados de seguridad. La autenticación de un cliente se realiza empleando alguno de los mecanismos de autenticación que soporte un servidor RADIUS donde se almacenan los usuarios autorizados
- WPA2 introduce un paradigma de seguridad Wi-Fi, basado en toda la tecnología desarrollada para WPA.
- Encaminamiento: Procedimiento por el que un paquete de información puede ser intercambiado entre cualquier par de equipos en una red de comunicaciones. La arquitectura TCP/IP define un funcionamiento de red de datagramas en su capa de red:
  - Cada paquete de información incorpora dirección origen y dirección destino.
  - En cada router se decide cuál es el siguiente salto que ha de realizar cada paquete.
- Protocolo IP. RFC 791: Define un sistema de numeración para identificar máquinas en una red. Define, también, un formato de paquete de nivel de red (interred) para el control del encaminamiento (cabecera IP)

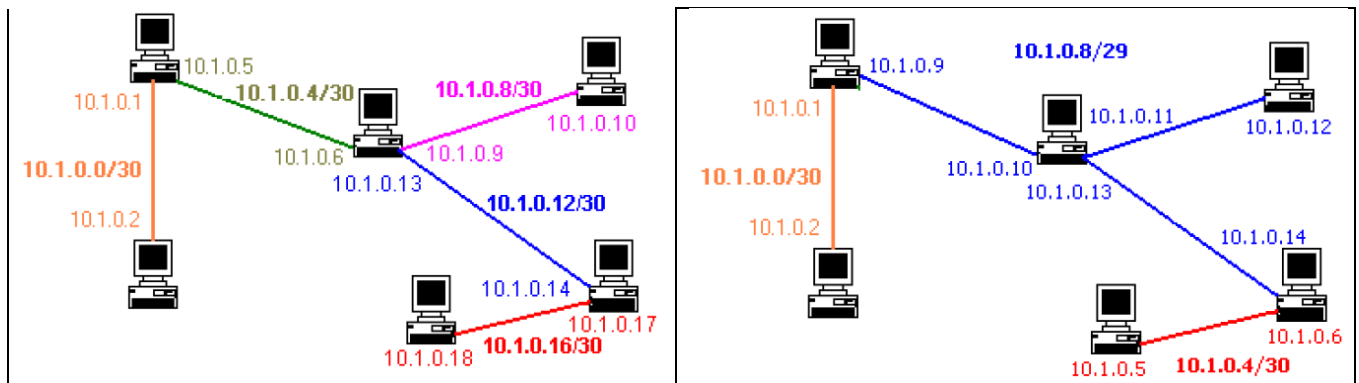
#### Direccionamiento IP



Clases de direcciones IP

- Redes de difusión: Todas las estaciones que comparten un mismo medio físico en una red de difusión tienen que tener asignada la misma dirección de red IP. La elección de la clase se determina dependiendo del número de máquinas en el segmento

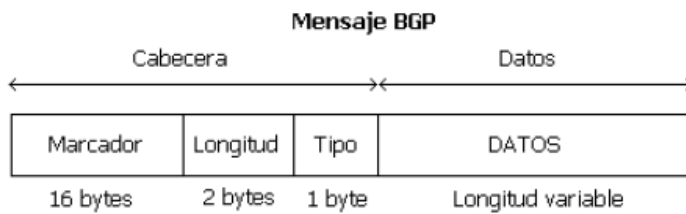
- Redes Punto a Punto: Las estaciones en los extremos de una red punto a punto tienen que tener asignada la misma dirección de red IP. Por cada enlace punto a punto se especifica una dirección de red IP. Para evitar la reserva innecesaria de direcciones IP, la máscara de red en una línea punto a punto se escoge para reservar el número de direcciones IP necesarias: 2 direcciones para máquinas, 1 para red y 1 para difusión.



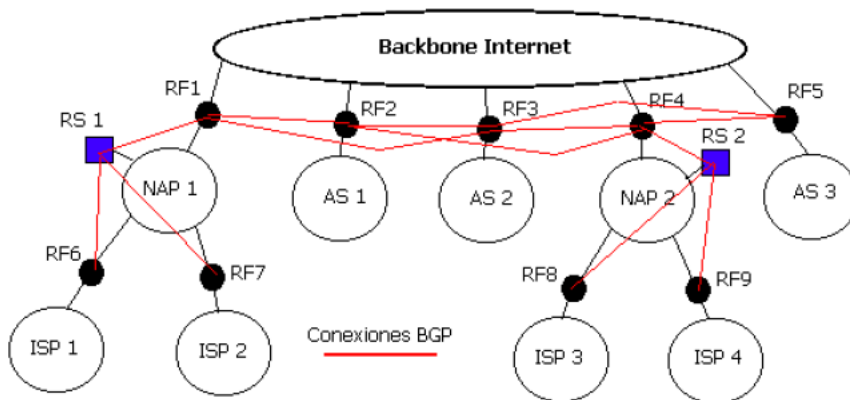
- Enlaces multipunto a punto: Ofrece varias rutas desde una única ubicación a varios lugares
- Dispositivos que precisan tablas de encaminamiento:
  - Estación, PC, host de la red: Precisa de una tabla de encaminamiento sencilla: una entrada para la red a la que pertenece y otra para la puerta de enlace.
  - Router( encaminador de la red ): Precisa de una tabla de encaminamiento compleja: necesita entradas en la tabla de encaminamiento para cada red que conoce y una para la puerta de enlace
- Una tabla de encaminamiento consta de una fila (entrada) por cada red IP que conoce el router. Se distinguen 3 tipos de entrada:
  - Entradas asociadas a redes conectadas directamente (la puerta de enlace es una dirección IP del router).
  - Entradas asociadas a redes alcanzables (la puerta de enlace es la dirección IP de un router).
  - Entrada de la puerta de enlace por defecto (la puerta de enlace es la dirección IP de un router).
- Una red de conmutación de paquetes presenta congestión si al aumentar el flujo de paquetes de entrada a la red (número de paquetes por segundo que entran en la red), disminuye el flujo de paquetes de salida (número de paquetes por segundo que salen de la red). Las causas son:
  - Routers con insuficiente capacidad de proceso. Detección: Es necesario monitorizar cuál es el porcentaje de uso de la CPU de los routers. Si el valor de utilización es superior al 60-70%, se hace necesario emplear un router con mayores prestaciones
  - Fragmentación de la información con el protocolo IP. los routers precisan más tiempo para encaminar la misma información que con un MTU más grande, ya que tienen que analizar más cabeceras IP. Detección: Es necesario verificar que los MTU de la red están elegidos adecuadamente y que la fragmentación se evita con mecanismos como la norma RFC 1191.
- Si en una red se detecta una situación de congestionamiento, hay una única solución para que la red no quede bloqueada: reducir el flujo de entrada de paquetes a la red. Esta estrategia es empleada por el protocolo TCP el cual es capaz de reducir su flujo de transmisión si no llegan los ACKs debido a la congestión
- Características de los core routers (routers del troncal):
  - Conocimiento de todos los destinos de Internet -> Tablas de encaminamiento grandes y complejas.
  - Simplificación de las tablas de rutas Conocimiento parcial de la red con rutas por defecto. Provocan inconsistencias (destinos inexistentes) y rutas no óptimas.
  - Gestión de las tablas de encaminamiento: Manual o automático
- 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.
- Protocolo de encaminamiento BGP (Border Gateway Protocol): Protocolo para el intercambio de información de encaminamiento entre sistemas autónomos. En cada sistema autónomo se especifica un router de frontera (o más, en general uno) que dialoga con los routers de frontera de otros sistemas

autónomos. La información de encaminamiento se intercambia empleando conexiones TCP (puerto servidor 179) entre routers de frontera.

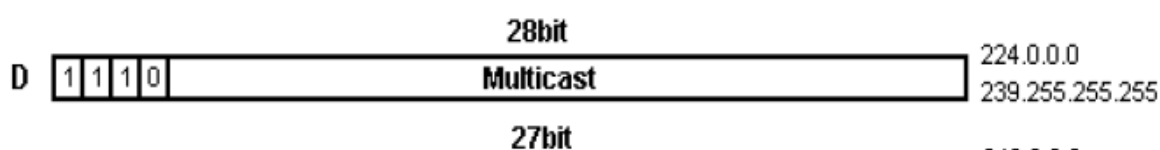
- El protocolo BGP se fundamenta en el establecimiento de una conexión TCP para el intercambio de diferentes mensajes BGP. Cada mensaje BGP consta de un paquete con cabecera y datos. La cantidad de datos y su formato depende del tipo de mensaje BGP.



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

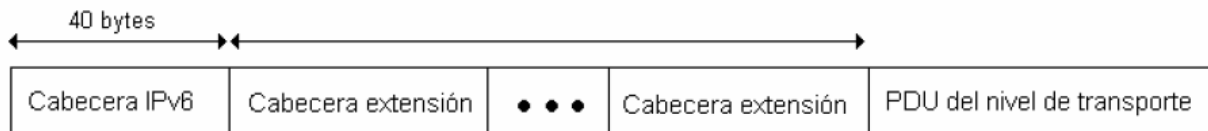


- BGP sólo informa de accesibilidad, no de rutas a seguir
- BGP establece conexiones entre pares de routers frontera
- BGP informa sobre destinos existentes y no existentes
- Protocolo de Información de Encaminamiento (RIP): Se fundamenta en un algoritmo de vector de distancia (Algoritmo de Bellman-Ford). Cada router dispone de una tabla con información de destinos y una métrica (número de saltos) para alcanzar el destino. Cada router propaga la información de sus rutas conocidas a través de mensajes en la red, y los routers que la reciben actualizan sus tablas si encuentran rutas más cortas a un mismo destino. Para cada entrada en la tabla de rutas (distancia, métrica) existe un temporizador (180 segundos). Si la ruta no es informada (distancia, métrica) de nuevo en ese tiempo, es eliminada, así evitamos bucles infinitos.
- Protocolo Abierto del Camino más Corto Primero (OSPF): se fundamenta en el denominado estado del enlace, asignando un coste dependiendo de las características del enlace. El conjunto de routers de una red que emplean OSPF conforman un grafo, donde se determinan las rutas más cortas entre cualquier par de nodos empleando el algoritmo de Dijkstra.
- Multicasting: Para este propósito está definida la clase D del direccionamiento IP, pudiendo establecer 228 direcciones de multidifusión, o lo que es lo mismo 228 direcciones de grupos de máquinas.

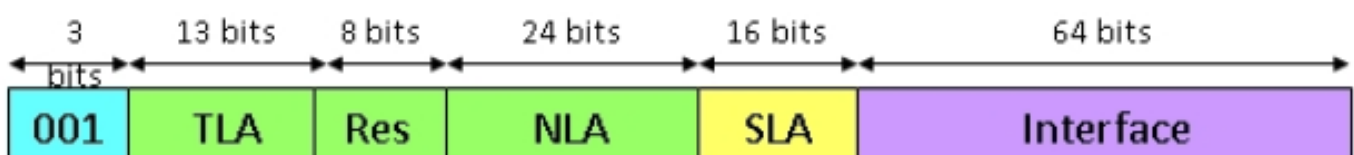




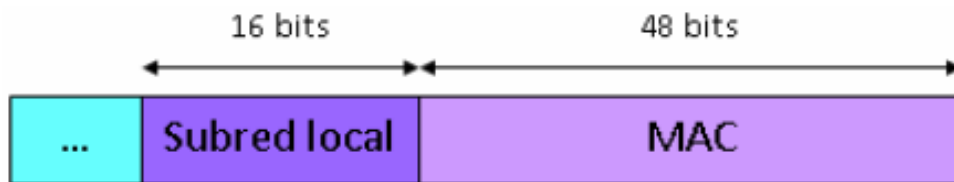
- Cada dirección de multidifusión tiene asociada una función específica, de forma que cada dirección de multicast identifica grupos de máquinas en Internet que llevan a cabo una función común.
- Cuando un paquete IP se envía a una dirección multicast ¿qué dirección de nivel de enlace se emplea?
- Si el nivel de enlace soporta multicasting (Ej: Ethernet) cada dirección IP de multicast tiene asociada una dirección de enlace de multicast.
- IGMP – Protocolo de Gestión de Grupo en Internet: Este protocolo, que al igual que ICMP funciona sobre IP estableciendo diferentes tipos de mensajes IGMP, permite la gestión del encaminamiento con multicasting.
- IPV4: La principal limitación que ha conducido a la introducción de una nueva versión de protocolo IP es la limitación en el direccionamiento IPv4 a 32 bits.
- IPv6 introduce direcciones IP de 128 bits, lo que supone disponer de aproximadamente  $6 \times 10^{23}$  direcciones por metro cuadrado de la superficie terrestre. La fragmentación provoca un efecto nocivo en el rendimiento de la red, por lo que IPv6 no permite la fragmentación de un paquete IP en un router intermedio.



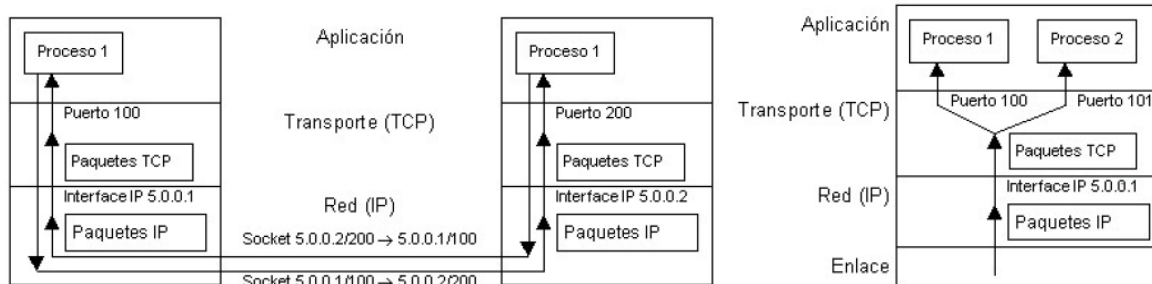
- Formato de la cabecera IPv6
  - Clase de tráfico: Permite establecer clases distintas de tráfico.
  - Etiqueta de flujo: Permite identificar flujos de paquetes entre dos aplicaciones origen y destino
  - Longitud carga útil: Tamaño en bytes de las cabeceras de extensión y la PDU de nivel superior.
  - Cabecera siguiente: Especifica qué cabecera sigue a la IPv6. Puede ser una cabecera de extensión o un protocolo de nivel superior (TCP, UDP).
  - Límite de saltos: Establece el número máximo de saltos de un paquete IP, al igual que en IPv4.
  - Dirección IP origen y destino: Especifica entre qué interfaces se intercambian los datos.
- Anidamiento de cabeceras extendidas en IPv6
- Cuando un dispositivo analiza un paquete IPv6 recorre todas las cabeceras existentes (IPv6 y extendidas) empleando el campo 'cabecera siguiente', hasta que encuentra la cabecera de nivel superior y envía los datos a la capa superior.
- IPv6 introduce un nuevo sistema de direccionamiento. Una característica fundamental de las direcciones IPv6 es que son dinámicas y únicas. La dirección IPv6 asignada a un interfaz es un valor de 128 bits combinación de la MAC del interfaz y del proveedor de acceso que emplea. Así, el proceso de encaminamiento es mucho más rápido en los routers, pues permite establecer jerarquías de direccionamiento más realistas como por operador, proximidad geográfica, etc.
- 3 tipos distintos de direcciones IP:
  - A) Direcciones de unidifusión (unicast): Identifican a un interfaz individual.
  - b) Direcciones de multidifusión (multicast): Identifica a un conjunto de interfaces que pertenecen a un grupo definido.
  - c) Direcciones de monodifusión (anycast): Identifica a un conjunto de interfaces que pertenecen a un grupo, pero el paquete sólo se entrega a la interfaz más cercana
- La notación de una dirección IPv6 se establece en 8 grupos de 4 dígitos hexadecimales separados por el símbolo ':' -> 2001:BA98:7654:3210:FEDC:BA98:7654:3210
- Es posible reducir la notación de una dirección IPv6 omitiendo los grupos que contengan ceros y
- empleando doble ':' -> 2001:BA98:0000:3210:0000:BA98:0000:3210 ó 2001:BA98::3210::BA98::3210



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



- Un dispositivo IPv4 sólo puede tener conectividad con dispositivos con IPv4, por tanto, si es necesaria conectividad IPv4-IPv6 entre dispositivos es necesario disponer de dos pilas de protocolo IP en paralelo.
- Capa de transporte:
  - TCP: Protocolo de control de la transmisión (fiable)
  - UDP: Protocolo de datagramas de usuario (NO fiable)
- Multiplexión de conexiones:



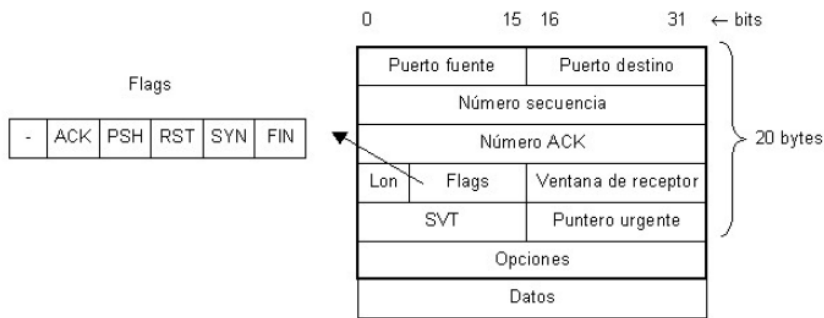
- La capa de transporte soporta múltiples conexiones entre un par de equipos empleando el número de puerto para separar los paquetes IP de cada conexión
- UDP: El protocolo UDP (User Datagram Protocol) está definido en RFC 768. Las características principales:
  - Sin conexión
  - Trabaja con paquetes o datagramas enteros, no con bytes individuales como TCP.
  - No es fiable. No emplea control del flujo ni ordena los paquetes.
  - Provoca poca carga adicional en la red
  - Un paquete UDP puede ser fragmentando por el protocolo IP
  - Admite utilizar como dirección IP de destino la dirección de broadcast

## Formato del paquete UDP

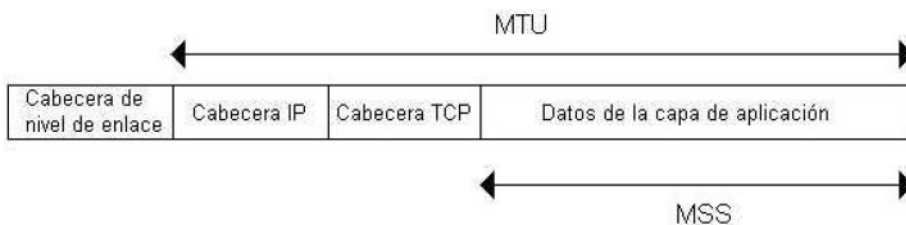


- TCP: El protocolo TCP (Transmission Control Protocol) está definido en RFC 793. Las características principales:
  - Trabaja con un flujo de bytes.
  - Transmisión orientada a conexión.
  - Fiable. Emplea control de flujo
  - Flujo de bytes ordenado

## Formato del paquete TCP



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



- Si la red no proporciona ningún mecanismo para controlar la congestión, éste ha de llevarse a cabo con los protocolos de la arquitectura de red. El protocolo de la capa de transporte TCP es un protocolo que presenta las características de:
  - a) Protocolo fiable con confirmación de paquetes.
  - b) Transmisión orientada a conexión.
  - c) Control del flujo de bytes.
- El control del flujo se realiza variando el tamaño de la ventana del receptor (campo window en la cabecera TCP):
  - a) Si la ventana del receptor aumenta, el emisor puede enviar más información sin esperar a recibir ACK (aumenta ventana del emisor).
  - b) Si la ventana del receptor disminuye, el emisor envía menos información sin esperar a recibir ACK (disminuye ventana del emisor). Caso límite: window=0.
- Si un segmento no llega al receptor o llega con errores, el receptor no enviará ACK. Los siguientes segmentos que envíe el emisor (hasta su tamaño de ventana máximo) se almacenarán en el buffer del receptor pero éste enviará ACK de la secuencia previa al paquete erróneo
- Cálculo del tiempo de espera de ACK. Algoritmo de Karn: El tiempo de espera de un ACK (Timeout) debe ser calculado de forma que:
  - Sea lo suficientemente grande para evitar que los retardos en la red no provoquen reenvíos innecesarios por retardos en el envío del ACK.
  - Sea lo suficientemente pequeño para que no haya periodos de inactividad en el envío de datos en la red.
- Control de la congestión en TCP. RFC 2581: La congestión en una red es una situación de retardo elevado en el envío de información, debido a la sobrecarga de encaminamiento en los routers de una red. Para reducir la congestión, TCP debe reducir la tasa de envío de datos, es decir reducir su ventana de emisor.
- Prevención de la congestión por decremento multiplicativo
- Esta técnica se fundamenta en la definición en el emisor de una nueva ventana denominada ventana de congestión, un valor en bytes al igual que la ventana del emisor.

- Recuperación de una situación de congestión. Algoritmo de inicio lento. Una vez que se evita la congestión y comienzan a llegar ACK's, el timeout vuelve a decrementarse y la ventana de congestión debería aumentar. La recuperación se realiza más lentamente. Para ello, el valor de la ventana de congestión se incrementa en un tamaño de MSS bytes, cada vez que el emisor recibe un ACK.