

Tema 1

1. Visión general de las redes de computadores

- {
 - Sistemas finales (host): pc, servidor, dispositivo móvil, teléfono móvil
 - Enlaces de comunicación: enlaces inalámbricos, enlaces cableados
 - Elementos de conmutación: router

Red de computadores:

Conjunto de sistemas finales (host) autónomos interconectados, se interconectan para intercambiar información mediante redes de comunicación

Red de comunicación:

Conjunto de enlaces y elementos de conmutación que hacen posible el intercambio de información entre sistemas finales, para poder intercambiar información, se utilizan los protocolos, algoritmos de encaminamiento, estrategias para gestionar el tráfico, métodos para detectar y corregir errores, mecanismos de seguridad, estándares...

Objetivos de las redes:

- Compartición de recursos
 - o Archivos, datos, programas, capacidad de cómputo...
 - o Independencia localización de usuarios y recursos
- Fiabilidad(QoS)
- Seguridad
- Ahorro económico
- Escalabilidad

2. Clasificación de las redes de computadores

Criterios de clasificación:

- Por la topología (disposición de los enlaces)
 - o Redes de topología regular: estrella, anillo, árbol, bus
 - o Redes de topología irregular: irregular
- Por la tecnología de transmisión
 - o Redes de difusión
 - También llamadas redes broadcast
 - Medio compartido por varios dispositivos
 - La información viaja acompañada de la dirección de destino
 - o Redes punto a punto
 - Conexiones entre pares de dispositivos
 - Para alcanzar el destino la información debe pasar por dispositivos intermedios
 - Almacenamiento temporal de los paquetes entre los nodos intermedios
- Por escala
 - o Redes PAN: Dispositivos en la misma habitación
 - Zona geográfica muy pequeña
 - Normalmente pertenece a un usuario que desea conectar distintos dispositivos
 - Normalmente se utilizan tecnologías inalámbricas y sistemas de difusión

compartir, fiável, seguro, barato y vaya +

-topología → regular → irregular
-tec. transmisión → difusión → punto a punto
-escala → PAN → habitación
 ↳ LAN → uni
 ↳ MAN → ciudad, país
 ↳ WAN → mundo
-mod. transp. info → circuitos
 ↳ mensaje
 ↳ paquetes
 ↓
 es mensaje dividido
 en partes

- Se necesita un mecanismo de control de acceso al medio compartido
 - No mucha capacidad de transmisión de datos
 - **Redes LAN:** Dispositivos en la misma habitación, edificio, campus
 - Zona geográfica de tamaño moderado
 - Normalmente pertenece a la entidad propietaria de los dispositivos conectados a la red
 - Utilización de sistemas distribuidos (normalmente)
 - Se necesita un mecanismo de control de acceso al medio compartido
 - Mayor capacidad de transmisión de datos
 - **Redes MAN:** Dispositivos en la misma ciudad, país
 - **Redes WAN:** Dispositivos en el mismo continente, planeta
 - Subred de comunicaciones: Líneas de transmisión, elementos de conmutación
 - Elementos de conmutación: IMP (procesadores de intercambio de mensajes)
 - IMPs: toman decisiones de encaminamiento mediante algoritmos de encaminamiento
 - Host: máquinas destinadas a ejecutar programas de usuario
- **Por el modo en el que se transporta la información**
- Redes de conmutación de circuitos
 - Se establece una ruta física dedicada entre los extremos de la comunicación
 - Todos los datos siguen el mismo camino
 - Si la comunicación se reitera más tarde la ruta podría ser distinta
 - Establecimiento de una conexión física cuando la llamada se ha realizado
 - Redes de conmutación de mensajes
 - No se establece una ruta dedicada inicialmente
 - El mensaje se transmite de un nodo a otro
 - El nodo recibe el mensaje completo, lo almacena, decide el siguiente nodo del camino hacia el destino y realiza el reenvío
 - Redes de conmutación de paquetes
 - Misma filosofía que la conmutación de mensajes
 - Se pone límite al tamaño de los datos: se fraccionan los mensajes en pequeñas unidades de información llamadas paquetes
 - Cada paquete puede seguir un camino diferente
 - Paquetes se meten en una cola para su posterior retransmisión

3. Protocolos y arquitecturas de protocolos (Para que los ordenadores se comuniquen)

- Puntos clave:

- **Mensajes enviados**
- **Acciones a realizar**
- **Respuestas a enviar**
- **Orden adecuado de los mensajes**

$m \rightarrow a \rightarrow r \rightarrow o$

rutas, acceso, cifrado..

- **Protocolo:** Es un conjunto de reglas que gobiernan el intercambio de información entre dos entidades (descubrimiento rutas, acceso a un medio compartido, cifrado de información...), lo define: → mensaje entre 2 PCs

- como se escribe →
- o Sintaxis: tipos y formato de los mensajes intercambiados (PDUs)
 - o Semántica: significado de los mensajes y acciones a realizar cuando...
 - Se transmite un mensaje (ej: arrancar un temporizador)
 - Se recibe un mensaje (ej: parar un temporizador)
 - Ocurre algún evento (ej: retransmitir un mensaje cuando vence un temporizador)
- que significa →
- Modelo de interacción: orden de los mensajes intercambiados

Normalización: garantiza la interoperación (todo el mundo lo use, los equipos respetan las normas)

- **Arquitectura de protocolos:** Es una estructura formada por el conjunto de módulos o capas que realizan las funciones comunicación entre entidades (Capa1-Capa5), proporciona servicios a las capas más altas.

- o Cada capa: 1 capa está formada: tareas relacionadas (conjunto de protocolos)

- Esta formada por un conjunto de tareas relacionadas (conjunto de protocolos)
- Proporciona servicios a la capa inmediatamente superior para que esta realice sus funciones
- Incorpora su propia información de control (tiene sus propias PDUs). Si son muy pequeños, no hace falta. Si son datos muy grandes, se parten. La IP de destino, lo leen todos los dispositivos, si es suya, se lo queda, si no lo es, lo envía

- o Protocolos y servicios

- Cada protocolo ofrece una serie de servicios, que son conocidos por la capa superior
- Ejemplos de tipos de servicio

{ Perdida de datos o no

- Fiable: el protocolo asegura que no se va a perder ninguna información que se le encargue enviar

- No fiable: el protocolo no garantiza nada, de cara la pérdida de la información por la red

{ Comunicación previa o no

- Orientado a conexión: las entidades que se van a enviar datos establecen una comunicación, antes de enviar dichos datos

- Datagramas: las entidades que se van a enviar datos no establecen una comunicación, antes de enviar dichos datos

- o Ventajas

- Asimilación de capas en componentes HW/SW
- Facilidad en el mantenimiento y la actualización de componentes de la red, cada capa encapsula los detalles concretos de como realiza las tareas

compacto

- o Inconvenientes

- Puede haber tareas duplicadas en varias capas (ej: control de errores, dos protocolos hacen lo mismo, corregir)

repetir cosas
↓
mucho espacio
ocupado,
sobrecarga
información

- Cada protocolo de cada capa añade información adicional a enviar por la red, sobrecarga (con las cabeceras, desperdicio de espacio, información redundante)

(Ni OSI ni TCP/IP)

navegador → servidor

no perder info

- Aplicación: el navegador tiene que entenderse con el servidor web
- Transporte: no quiero que se pierda ningún dato que se envíen el navegador y el servidor web (se hace petición get, el servidor lo entiende y la información que devuelva sea completa y en orden de aplicación)
- Red: hay que encaminar los datos a través de la red para que lleguen a las máquinas donde se ejecutan el navegador y el servidor web (capa para decidir el camino de ida y vuelta)
- Enlace: el PC y el servidor tiene que poder enviar los datos dentro de su red local hasta el punto de salida exterior (en vez de transporte origen destino, salto a salto de routers)
- Físico: los bits tienen que fluir de alguna manera por los enlaces

- Arquitectura de protocolos TCP/IP

- Capa de aplicación: Aplicaciones usuario, unidad básica de información: mensaje, protocolos HTTP, FTP, SMTP, DNS... (genera mensajes)
- Capa de transporte:

- Transporta los mensajes de las aplicaciones entre los sistemas finales (proporciona comunicación extremo-extremo)

- Puede controlar el flujo de datos entre los sistemas finales

- Capa común para todas las aplicaciones de usuario

- Direcciona las aplicaciones mediante puertos

- Protocolo: TCP, UDP

- Unidad básica de información: segmentos (TCP) o datagramas (UDP)

↳ direcc. med. puertos

- Capa internet:

- Encamina los paquetes a través de varias redes

- Controla la gestión de la red

- Permite la interconexión de redes de distinta naturaleza

- Direcciona las máquinas mediante direcciones IP

- Unidad básica de información: datagrama

- Protocolos: IP (IPv4/IPv6), ICMP ...

- Internet → IP, ICMP

- Capa de acceso a la red:

- Intercambia datos entre cada par de nodos (host, routers) que forman parte de la ruta entre el origen y el destino

- Controla el flujo de datos

- Se encarga de encaminar la información dentro de las redes LAN

- Direcciona las maquinas mediante direcciones físicas (ej: direcciones MAC)

- Unidad básica de información: trama

- Protocolos: Ethernet, Wifi, Bluetooth, Token Ring ...

- Acceso red → Ethernet,

wifi,

Bluetooth ...

- Física

↳ saltos

↳ bits a

señales

↳ independe del

medio

de transmisión

- Capa física:

- Transporta la información

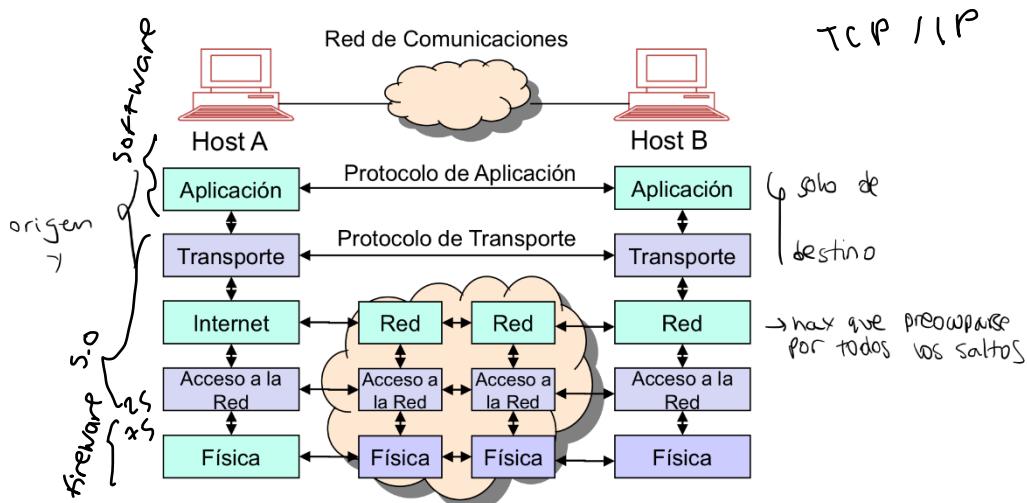
- Especifica la naturaleza de las señales a enviar, la codificación de los bits en señales ...
 - Es dependiente del medio de transmisión
- **Modelo OSI (Open Systems Interconnection)**
- Desarrollado por la Organización Internacional de Estandarización (ISO) (capa de aplicación)
 - Capa de presentación: define el formato de datos a intercambiar (sintaxis y → como se esccribe)
 - → semántica), comprensión de datos, criptografía ...
 - Capa de sesión: tareas de sincronización para el intercambio de datos, → restaur. establece puntos de restauración de sistema y recuperación de datos → recup. sincron.
 - Todo esto lo realiza la aplicación, si es que lo necesita

aplicación
que signif.

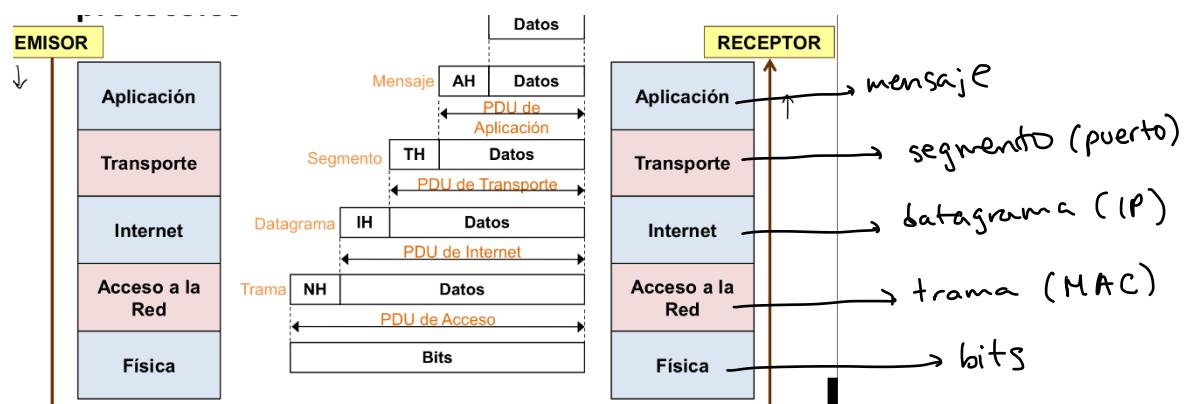
- **Comparativa de las arquitecturas:**

- OSI
 - Programas software: Aplicación, presentación, sesión (50/100)
 - Sistema Operativo Software: Sesión (50/100), transporte, red
 - Tarjeta de red firmware: enlace de datos, física
- TCP/IP
 - Programas software: Aplicación
 - Sistemas operativos software: Transporte origen-destino, internet, acceso a la red (25/100)
 - Tarjeta de red firmware: Acceso a la red (75/100), física

- **Funcionamiento de la arquitectura de protocolos**



Las cabeceras añaden información y el mensaje es mayor



- Direccionamiento en la arquitectura
 - o Aplicación
 - o Transporte
 - Puerto origen: aplicación que envía los datos
 - Puerto destino: aplicación que va a recibir los datos
 - o Internet
 - IP origen: host que envía los datos
 - IP destino: host que va a recibir los datos
 - o Acceso a la red
 - MAC origen: máquina origen del salto de que van a dar los datos
 - MAC destino: máquina destino del salto que van a dar los datos
 - o Física
 - Ningún tipo de dirección

- Elementos de interconexión en las arquitecturas

- o Router (Internet): encamina datagramas examinando su IP (no pertenecen a la misma red), comprueba que la dirección MAC es suya, luego comprueba si la dirección es suya o alguna que el conoce
 - Casa puerto del router pertenece a una red física diferente y tiene su propia dirección IP y dirección MAC
- o Switch (Acceso a la red) : encamina tramas examinando si dirección MAC (los dispositivos conectados pertenecen a la misma red), lo retransmite por una o varias salidas, interpretan el mensaje, es capaz de leer la cabecera de acceso a la red, comprenden las MAC y por eso puede saber porque salida sacarlo
 - Todos los puertos del switch pertenecen a la misma red física y cada uno de ellos tiene su propia dirección MAC (aulario polivalente switches al router)
- o Hub (Física): retransmite bits por todos los puertos, un ladrón, permite conectarlo todo con todo, si llegan dos a la vez imposibilita la conexión

IP, mac suya

→ MAC, donde sacarlos

→ bits, todo con todo

- Ejemplo:

- o Aplicación
 - Protocolo HTTP: Get <https://www.epigijon.uniovi.es>
 - Lo ultimo que hace: El servidor atiende el mensaje entrante y genera el mensaje saliente.
 - Mensaje saliente: HTTP 200 OK datos a enviar
 - Vuelta a empezar
- o Transporte
 - Protocolo TCP:
 - Cabecera del segmento:
 - o Puerto origen: 3250 (navegador) (podría ser cualquier otro)
 - o Puerto destino: 80 (servidor web) (HTTP o HTTPS)
 - Cuerpo del segmento: mensaje
 - Se encapsula el mensaje en el segmento TCP

Mensaje

Segmento

- Cuando vuelve de internet la ultima vez: El servidor busca la aplicación con puerto 80 para entregarle el mensaje, se desencapsula el mensaje

- Internet

- Protocolo IP *ICMP...*

- Cabecera del datagrama:
 - IP origen: 193.16.45.3 (mi PC)
 - IP destino: 156.35.189.45 (servidor) (se obtiene con el DNS)
 - Se encapsula el segmento TCP en el datagrama IP
 - Cuando vuelve del acceso a la red: el router busca el puerto por el que debe retransmitir el datagrama
 - Cuando vuelve del acceso a la red de nuevo: el servidor comprueba que su dirección IP es la dirección IP destino, se desencapsula el segmento TCP

- Acceso a la red

- Protocolo Ethernet *wifi, bluetooth...*

- Cabecera de la trama:
 - MAC origen: 0009.7C90.E79A (mi PC)
 - MAC destino: 0001.4288.04A2 (mi router)
 - Cuerpo de la trama: datagrama IP
 - Mi PC averigua la dirección MAC de mi router
 - Se encapsula el datagrama IP en la trama Ethernet
 - *El router comprueba que la MAC del puerto por el que recibe la trama es la MAC destino*
 - *Se desencapsula el datagrama IP*
 - Cabecera de la trama:
 - MAC origen: 0050.0FC2.A12D (mi router)
 - MAC destino: 0060.4729.8FF3 (router vecino)
 - El router averigua la MAC del router vecino
 - Se encapsula el datagrama IP en la trama Ethernet
 - Cabecera de la trama:
 - MAC origen: 0030.F269.0E3B (router)
 - MAC destino: 0060.2F80.BE1E (servidor)
 - El servidor comprueba que su MAC es la MAC destino
 - Se encapsula el datagrama IP

frame

Tema 2: Nivel Físico

→ bits a señales
↳ depende del medio de transporte

1. Introducción

- Funciones de la capa física

- Mover los bits por el enlace
- Sincronizar la transmisión entre emisor y receptor
- Especificar la naturaleza de las señales a enviar
- Definir la codificación de los bits en señales
- Especificar el tipo de transmisión
- Caracterizar el medio de transmisión
- Definir el formato y las funciones de los pines de un conector (como poner la información en el medio)

- Tipos de datos

- Analógicos: Toman cualquier valor en un intervalo continuo (ej: señal de voz)
- Digitales: Toman valores discretos (ej: número de alumnos matriculados)

- Tipos de señales

- Analógicas: Su intensidad varía suavemente en el tiempo (sin discontinuidades)
- Digitales: Su intensidad se mantiene constante en el tiempo, tras el cual pasa a otro valor constante (0 o 1, no hay datos intermedios)

- Datos y señales

- Cualquier tipo de dato se puede transmitir con cualquier tipo de señal
- Ejemplos:
 - Datos analógicos a señal analógica: teléfono, radio
 - Datos digitales a señal analógica: módems, mandos
 - Datos analógicos a señal digital: cuantificación → analogica a digital!
 - Datos digitales a señal digital: usb, ficheros

- Tipos de transmisión:

- Simplex (solo recibe): la transmisión se produce en un único sentido, televisión, radio...
- Semidúplex (recibe o envía): la transmisión se produce en ambos sentidos, pero no a la vez, walkie-talkie, internet
- Dúplex (recibe y envía): la transmisión se produce en ambos sentidos a la vez, teléfono, videoconferencia...

- Ruido: Señales adicionales que se insertan entre el emisor y el receptor, efecto del ruido en una señal digital (puntos concretos de error)

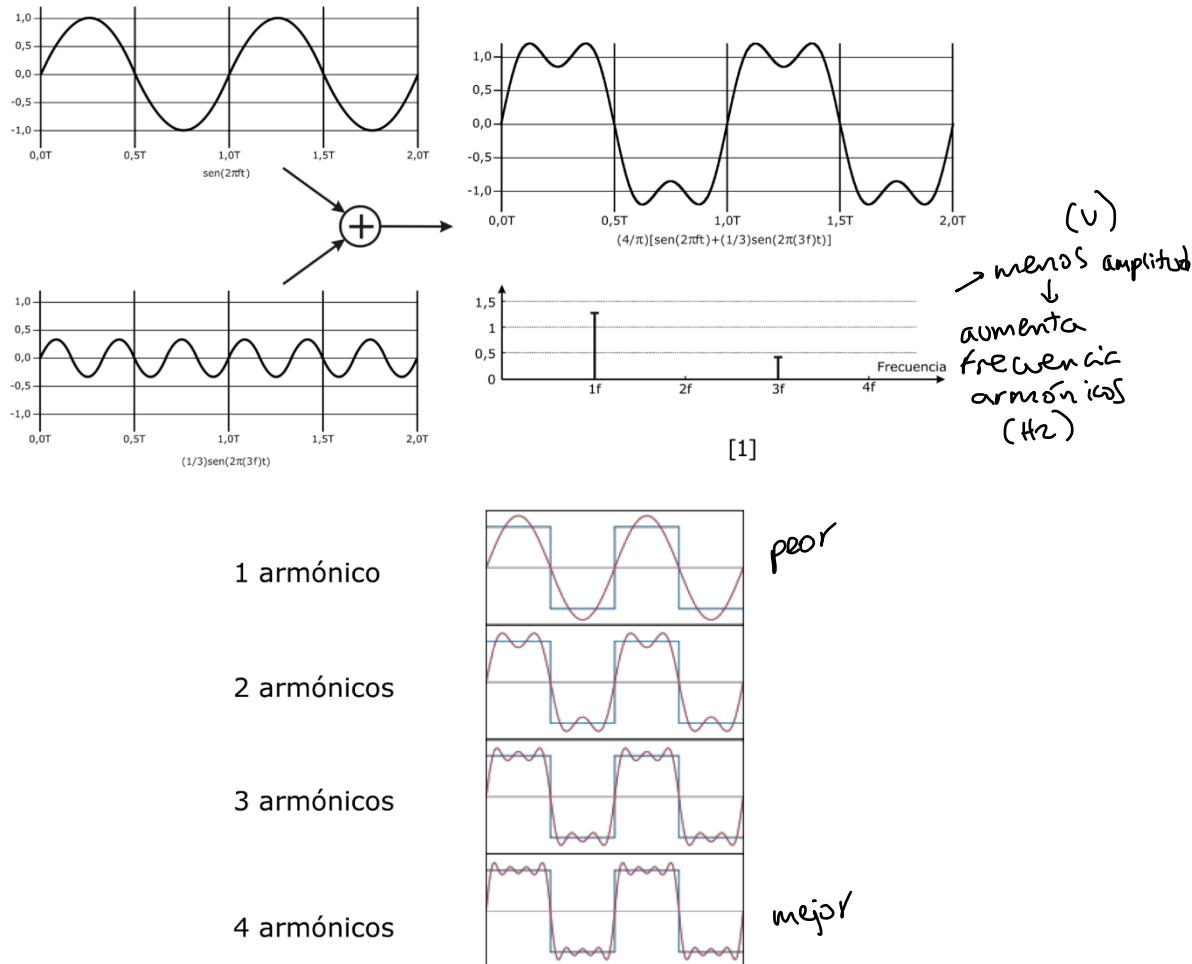
2. Señales en el dominio de la frecuencia

- Conceptos básicos

- Métodos de análisis de una señal
 - Dominio del tiempo: variaciones temporales de la señal, se analizan los parámetros, amplitud, frecuencia y base ↗ fase
 - Dominio de la frecuencia: se descompone la señal en componentes sinusoidales de diferentes frecuencias (análisis de Fourier), se puede separar por senos y cosenos, se analiza la frecuencia y amplitud de los componentes

(v) (Hz)
Amplitud, frecuencia, fase
↑
análisis fourier

- **Características de la señal sinusoidal**
 - Amplitud de pico (A): tensión máxima, se mide en voltios
 - Frecuencia (f): tasa de cambio de la señal, se mide en hertzios (cambios por segundo)
 - Fase (Φ): desplazamiento de la señal
- **Análisis en el dominio de la frecuencia**
 - Análisis de Fourier
 - Cualquier señal periódica puede expresarse como una suma infinita de señales sinusoidales, llamadas armónicos
 - Cada armónico tiene una frecuencia múltiplo de la frecuencia de la señal original (frecuencia fundamental)
 - A medida que aumenta la frecuencia de los armónicos, disminuye su amplitud
 - Una vez se ha descompuesto la señal, se pueden enviar los armónicos por el medio de transmisión, cuantos más armónicos se utilicen, más se aproximará la suma resultante a la señal original
 - Para aproximarse a una onda cuadrada, cuantos más armónicos, mejor



- **Características principales**
 - Espectro: conjunto de frecuencias que constituyen una señal \rightarrow frecuencias de 1 señal
 - Ancho de banda absoluto: anchura teórica del espectro \rightarrow ancho de 5 teorico

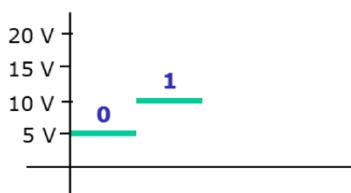
real

- **Ancho de banda efectivo:** banda de frecuencias que contiene la mayor parte de la energía. Cuando se habla de ancho de banda, se habla de este
- **Velocidad de transmisión:** numero de bits que se trasmiten en un segundo por medio de transmisión
- Relación entre el ancho de banda y la velocidad de transmisión: a mayor ancho de banda, mayor es la velocidad con la que se puede transmitir, cuanto mayor sea la velocidad que se necesite, mas ancho de banda hará falta
+ velocidad, + ancho de banda

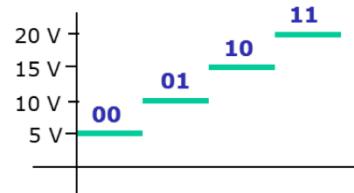
3. Capacidad del canal (bps)

- **Capacidad del canal:** tasa máxima de información que se puede enviar por la línea, se mide en bits/seg (bps)
- **Criterio de Nyquist:** Capacidad del canal sin ruido $C=2 \cdot B \cdot \log_2 M$, donde B es el ancho de banda en Hz del medio y M es el numero de niveles de señal

2 elementos de señal



4 elementos de señal



$B \rightarrow$ ancho banda \rightarrow Hz
 $M \rightarrow$ n° niveles de señal
 $SNR \rightarrow$ relación señal-ruido

alta calidad,
menos rep.
intermedios

4. Medios de transmisión

- Tipos de medios

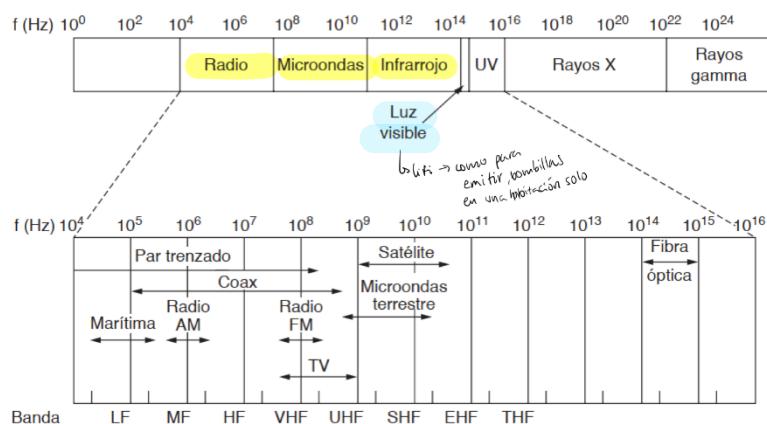
- **Guiaido:** la señal esta confinada a un camino físico
 - Par trenzado: hilos de cobre aislados y entrelazados de forma helicoidal, capacidad del orden de decenas de Gbps en 1km de distancia, barato, utilizado en redes de área local
 - Apantallados (STP, shielded twisted pair)
 - No apantallado (UTP, unshielded twisted pair)
 - Cable coaxial: Hilo protector y malla separados por un aislante y protegidos por plástico, capacidades de cientos de Mbps en distancias de kms, utilizado en televisión, enlaces de larga distancia...
 - Fibra óptica: contiene un núcleo y un revestimiento de cristal/plástico con distintos índices de refracción, esta forrado con una cubierta aislante, capacidad de Gbps en miles de kms, tradicionalmente usado en enlaces de larga distancia, aunque su uso está cada vez más extendido

+ potente,
+ caro,
+ alcance

- No guiado: la señal no está confinada
 - Ondas de radio
 - Señales con frecuencias desde 1Mhz hasta 1Ghz
 - Se propaga en todas las direcciones
 - Proporcionan poco ancho de banda a gran distancia (frecuencias bajas, largas distancias)
 - Tienen un coste alto debido a sus "bajas" frecuencias, pero es asumible por la gran cantidad de usuarios
 - Utilizado en la distribución de radio, televisión, telefonía móvil...
 - Microondas
 - Señales con frecuencias desde 1Ghz hasta 300Ghz
 - Se pueden utilizar antenas direccionales para propagar en forma de haz
 - Mucho ancho de banda a gran distancia
 - Se pueden utilizar antenas orientadas tanto en transmisión como en recepción
 - Pueden usarse con satélites (1-10Ghz) o en la tierra (1-40Ghz)
 - Utilizadas en enlaces de larga distancia, televisión por satélite...
 - También se pueden utilizar antenas omnidireccionales
 - Ancho de banda medio a media distancia
 - Utilizando en WiFi (2, 4), redes locales (5 móviles)
 - No se necesitan antenas orientadas (ya que va a todas direcciones)
 - Bajo coste
 - Infrarrojos (ya no pueden ser bidireccionales)
 - Señales con frecuencias desde 300Ghz hasta 400Thz
 - La señal se propaga en línea recta y es reflejada/absorbida por las paredes (rebota, mando garaje, no practico wifi "estar apuntando al router")
 - Poco ancho de banda y a poca distancia
 - Utilizado en conexión de dispositivos, redes locales ...
 - Bajo coste

+ potente,
poca distancia,
+ barato)

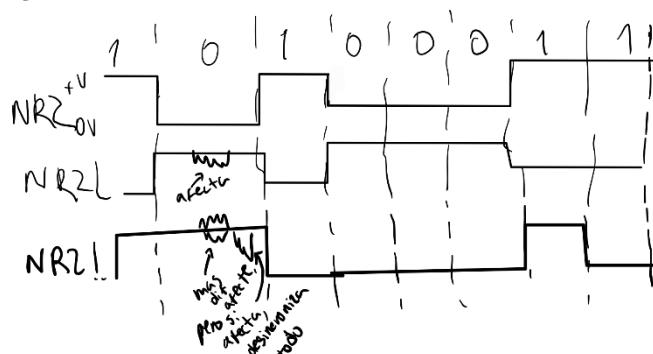
- Espectro electromagnético: relación fundamental:
 - frecuencia * longitud de onda = velocidad de la luz



5. Esquemas de codificación y modulación

- Codificación

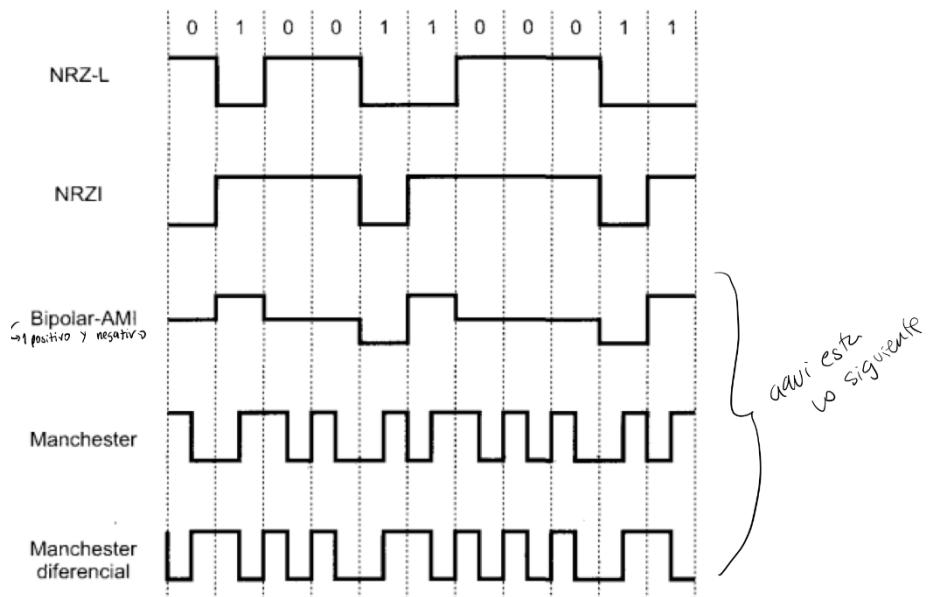
- Enviar datos analógicos o digitales mediante señales digitales
- Si es necesario, la señal se convierte a digital
- Se puede hacer en banda base o paso banda
- Datos digitales a señal digital
 - Cada bit se envía codificado en un elemento de la señal
 - Diferentes alternativas
 - Non Return to Zero (NRZ): Utiliza 0 para representar el 0 y un voltaje positivo para representar el 1
 - Non Return to Zero (NRZ-L): Utiliza 0 para representar el 1 y un voltaje positivo para representar el 0
 - Non Return to Zero (NRZ-I): Cuando aparece un 1, el voltaje de la señal varía. Más robusto ante el ruido, pero muy sensible ante fallos



- Binario multinivel: Bipolar AMI (Alternate Mask Inversion)
 - Utiliza más de dos niveles de señal
 - Se utiliza un voltaje nulo para representar el 0
 - Se utiliza un voltaje +V de forma alterna para representar el 1
 - No hay problemas de sincronización para detectar cadenas largas de 1
 - Sigue existiendo dicho problema para las cadenas largas de 0s
 - Ayuda a detectar posibles errores
- Códigos bifase:
 - Manchester:
 - Transición en mitad del intervalo de duración del bit
 - La transición sirve como procedimiento de sincronización y de transmisión de datos:
 - 0: transición de alto a bajo en mitad del intervalo
 - 1: transición de bajo a alto en mitad del intervalo

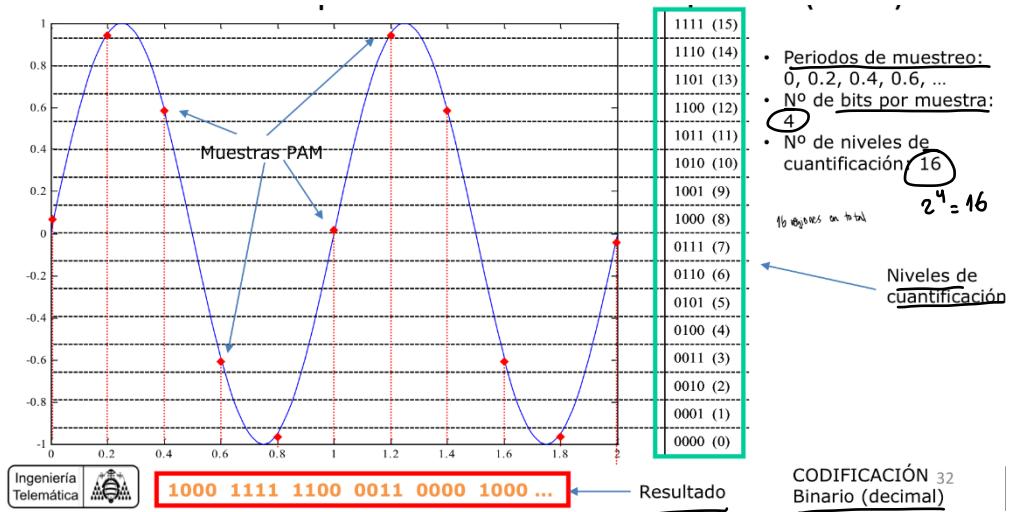
- Manchester diferencial:

- La transmisión a mitad del intervalo se utiliza tan solo para proporcionar sincronización
 - 0: transición al principio del intervalo del bit ↳ cambio
 - 1: Ausencia de transición al principio del intervalo del bit
- Es un esquema de codificación diferencial



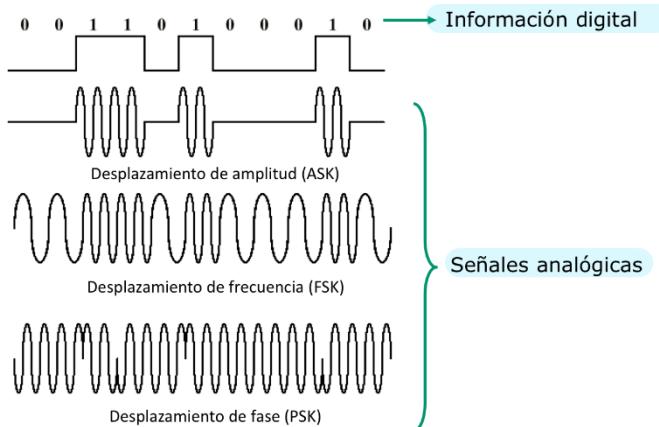
- Datos analógicos a señal digital (cuantificación)

- Digitalización: transformación de datos analógicos en señales digitales
- Modulación por codificación de impulsos (PCM) (solo saberlo y entenderlo)
 - Determinar la frecuencia de muestreo, teorema del muestreo de Nyquist: Si una señal se muestrea a intervalos regulares de tiempo con una frecuencia mayor que el doble de la frecuencia más alta de la señal, las muestras obtenidas contienen toda la información de la señal original
 - Determinar el nº de bits que va a codificar cada muestra, determina el nº de niveles de cuantificación
 - Muestra la señal a intervalos regulares, según el teorema de muestreo de Nyquist, se obtienen las muestras PAM (muestras analógicas) ↳ habitación
 - Codificar cada PAM con el código binario que le corresponde a su nivel de cuantificación
 - Problemas: redondeo, calidad de algo infinito a finito



Modulación

- Envío de datos analógicos o digitales mediante señales analógicas
 - Es necesario adaptar la señal a una representación analógica
 - Se suele realizar en paso banda
 - **Datos digitales a señal analógica**
 - Los datos se codifican mediante una señal llamada moduladora
 - La señal modulada modifica los parámetros de la señal portadora
 - Técnicas
 - Desplazamiento de amplitud (ASK)
 - Desplazamiento de frecuencia (FSK)
 - Desplazamiento de fase (PSK)
 - Señal moduladora -> Proceso -> Señal
 - Señal portadora -> de modulación -> modulada
 - Desplazamiento de amplitud: Los valores binarios se representan mediante dos amplitudes de portadora
- $$s(t) = \begin{cases} A * \cos(2\pi f_c t) & 1\text{ binario} \\ 0 & 0\text{ binario} \end{cases}$$
- Desplazamiento de frecuencia: Los valores binarios se representan mediante dos frecuencias de portadora
- $$s(t) = \begin{cases} A * \cos(2\pi f_1 t) & 1\text{ binario} \\ A * \cos(2\pi f_2 t) & 0\text{ binario} \end{cases}$$
- Desplazamiento de fase: La fase de la señal se desplaza para representar los datos
- $$s(t) = \begin{cases} A * \cos(2\pi f_c t + \pi) & 1\text{ binario} \\ A * \cos(2\pi f_c t) & 0\text{ binario} \end{cases}$$



- **Datos analógicos a señal analógica**

- Razones para modular las señales analógicas:

- Desplazar el espectro de frecuencias de la señal a una más adecuada para la transmisión, a mayor frecuencia, mayor velocidad de transmisión

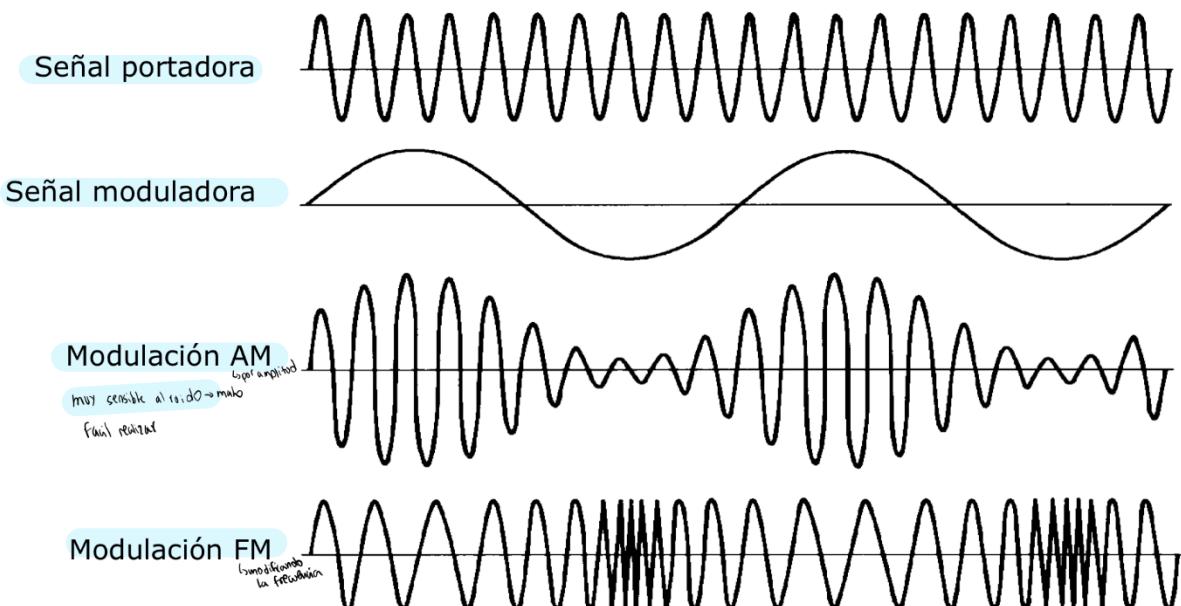
- Permite la multiplexación por división de frecuencias

- Tipos de modulación:

- En amplitud (AM) amplitud → facil de realizar, muy sensible al ruido
- En frecuencias (FM) frecuencia forse
- En fase (PM)

Señal moduladora -> Proceso de modulación -> Señal
Señal portadora -> ->modulada

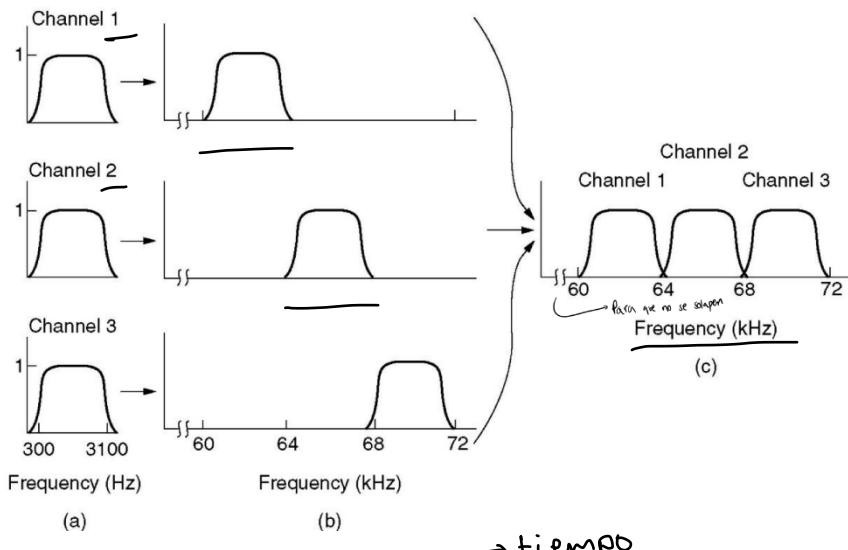
mayor frecuencia
↓
veloc.



6. Multiplexación

- **Definición:** Técnica que permite la transmisión de datos procedentes de varias fuentes sobre un mismo medio de transmisión mismo medio de transmisión diferentes fuentes
- **Objetivo:** Aprovechar al máximo las capacidades del medio compartido, las capacidades de los canales suelen ser muy superiores a las que necesita un solo usuario
- n entradas-MUX-----1 enlace, n canales-----DEMUX-n salidas
- **Multiplexación por división de frecuencias (FDM)**
 - Requisitos: Señales analógicas (independientemente de su contenido), ancho de banda del medio > suma del ancho de banda de las señales de las fuentes
 - Procedimiento: Modular cada señal de entrada con una señal portadora distinta

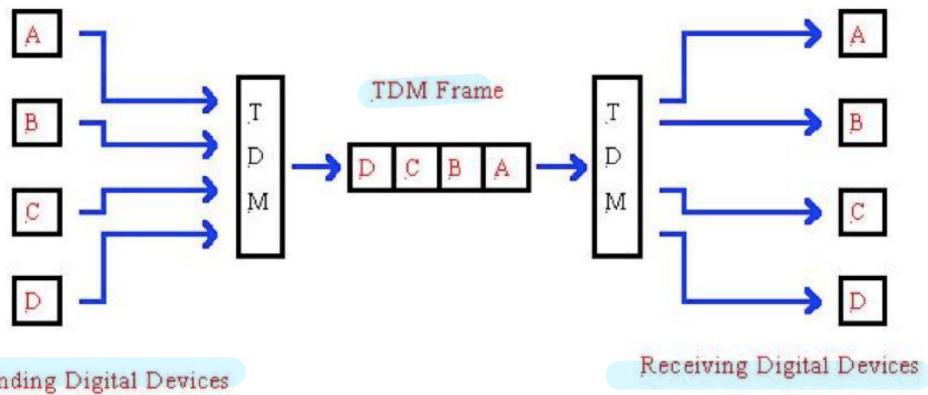
(FDM) División de frecuencias: para que no se solapen



→ tiempo

- Multiplexación por división en el tiempo síncrona (TDM)

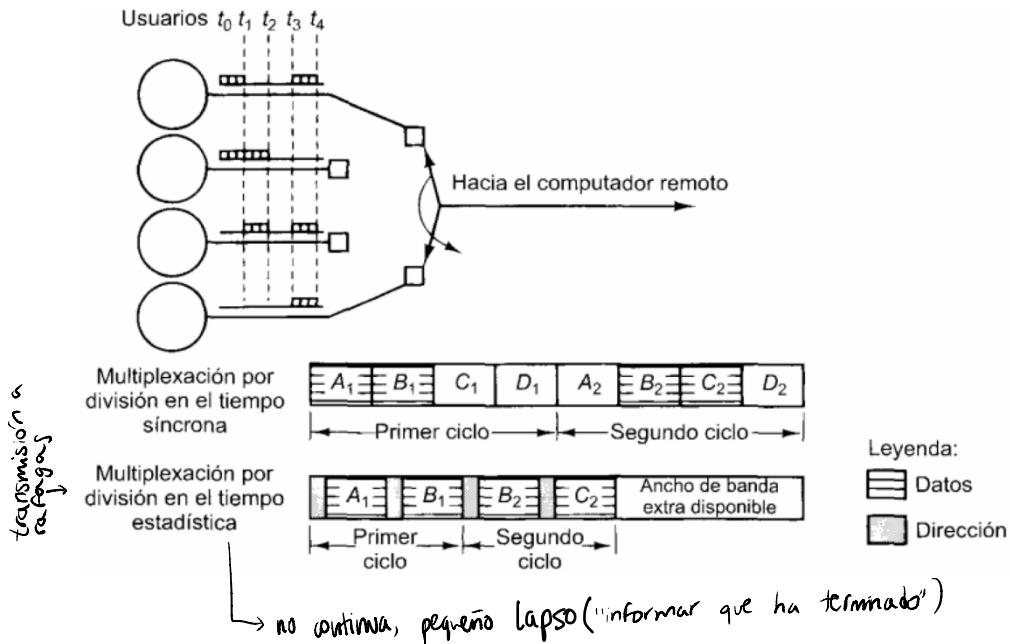
- Requisitos: Señales que representen datos digitales, velocidad de transmisión del medio > suma de las velocidades de transmisión de las fuentes
- Procedimiento: División del tiempo en ranuras temporales, las ranuras temporales se pre-asignan y fijan a las distintas fuentes, las ranuras temporales se asignan, incluso, si no hay datos, las ranuras temporales no se tienen que distribuir de manera igualitaria entre las fuentes
- Inserción de los datos de las fuentes en las ranuras temporales
- Mezcla en el tiempo varias señales que representan datos digitales



→ Tiempo estática

- Multiplexación por división en el tiempo estadística (STDM)

- Si alguna de las fuentes no transmite en FDM o TDM se desperdicia ancho de banda
- Con STDM se distribuyen las ranuras temporales de forma dinámica (se puede transmitir)
- El multiplexor sondea que fuentes tienen datos y se llena las ranuras con unas pocas fuentes
- Si hay exceso de datos, estos se guardan en buffers, peligro de congestión



Tema 3: Nivel de enlace (trama) (MAC)

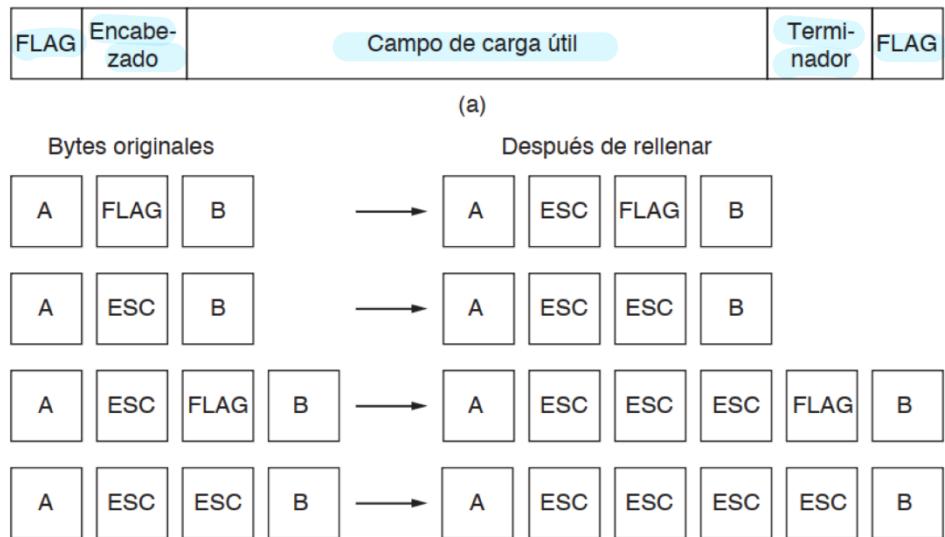
1. Introducción

- **Funciones de la capa de enlace**
 - Realizar un transporte de datos libre de errores salto a salto entre dos nodos unidos por un enlace
 - Proporcionar una interfaz bien definida a la capa de red
 - Delimitación de las tramas
 - Detectar y corregir los errores de transmisión (mediante software, gestionar lo que hay, salto a salto, router a PC)
 - Controlar el flujo para no saturar a los receptores (entre los extremos del enlace, se haga en un tiempo correcto)
 - Controlar el acceso al medio cuando este sea compartido, decir cuando se puede transmitir información o está ocupado (como compartir, comparto del medio)
 - Gestionar el envío de las tramas de forma directa por el enlace, direcciones MAC (como el DNI de un ordenador único y no se puede cambiar)

2. Delimitación de tramas

- **La unidad básica de transmisión a nivel del enlace son las tramas** (acotar que es el H1, H2), no coinciden necesariamente con el tamaño de los paquetes de nivel superior
- Es necesario acotar de alguna forma, el inicio y final de la trama
- Técnicas más habituales de delimitación: relleno de bytes o inserción de caracteres, inserción de bits, violaciones de código
- **Inserción de caracteres** (cabeceras "ya está incluida" para trabajar con la información) ↳ ↲
 - Se emplean una o más caracteres para indicar el comienzo o el fin de la trama
 - Suelen ser caracteres ASCII (8 bits principio y final) (ñHolañEspa\ñañespacio)

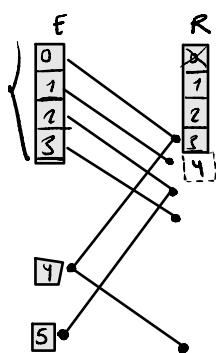
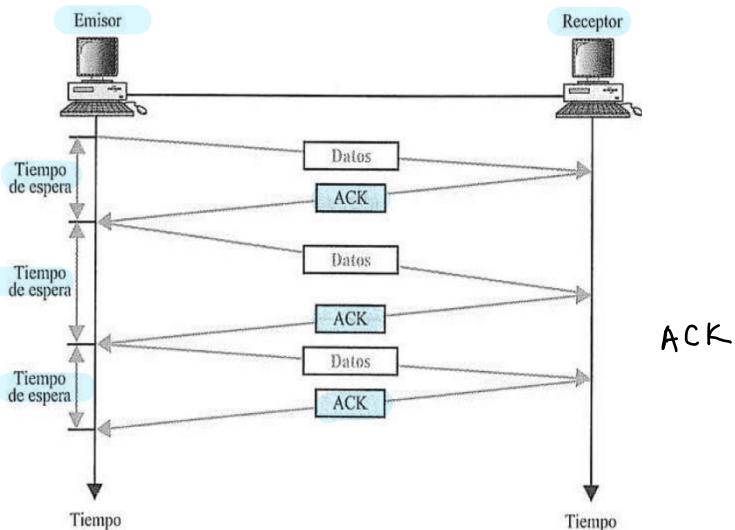
- Si alguno de los caracteres aparece en la propia trama, se inserta un carácter de escape, para indicar que no es el final de la trama
- En el caso de que apareciera un carácter de escape, se añadiría otro previamente ↴ ↵



- **Relleno de bits → S ons**
 - Se utiliza una secuencia de bits para marcar el inicio o fin de la trama
 - Ejemplo HDLC (High-level Data Link Control)
 - Tramas delimitadas por 0111110
 - Si aparecen cinco 1s consecutivos en la trama, se añade un 0 a continuación
 - El receptor elimina los 0s en el destino
- **Violaciones de código → junto con la capa física, voltajes, codificación**
 - Es un método que funciona de forma conjunta con la capa física (nivel de enlace influye directamente la capa física, se intenta evitar)
 - Se aprovechan elementos no utilizados de la capa física como señales de limitación de trama, voltajes diferentes a los utilizados para enviar la señal (10V y como máximo 5V), variaciones sin asignar en la codificación

3. Control de flujo

- **Evitar que el emisor sature al receptor**
 - Si la velocidad de envío es demasiado elevada, el receptor puede empezar a descartar tramas, se puede solicitar al emisor que no envíe más tramas, indicar que envíe más despacio, preguntar por la cantidad de memoria libre al receptor
 - Esta tarea puede llevarse a cabo también en capas superiores, como TCP en el nivel de transporte ↳ segmento (puerto)
- **Parada y espera**
 - Protocolo sencillo válido en un medio sin errores
 - Cuando el emisor manda una trama, ha de esperar el asentimiento para transmitir la siguiente
 - Uso del canal muy bajo (más tiempo esperando que enviando)



- Ventana deslizante

- Mismo funcionamiento que en el caso de TCP en el nivel de transporte
- Las tramas se etiquetan con un numero de secuencia **se etiquetar las tramas**
- Es la base de funcionamiento de las técnicas ARQ, que se estudiarán más adelante **ARQ**
- Permite una utilización mucho más elevada del canal

4. Control de errores

- **Transmitir por un medio ruidoso degradada las tramas (corregir para no reenviar)**
 - Se pueden producir dos situaciones
 - Corrupción de bits: La trama llega, pero algunos bits no son correctos → **una parte**
 - Perdida de tramas: No llega nada de la trama → **no llega nada**
 - Es necesario controlar los posibles errores y corregirlos cuando sea posible
 - Dependiendo del medio de transmisión utilizada, puede ser mas interesante detectar y retransmitir, que corregir
- **Numeración de tramas (Detectar errores)**
 - El transmisor etiqueta cada trama con un numero de secuencia (numera las tramas, para saber si han llegado todas)
 - El receptor comprueba los números de trama recibidos (detectar tramas repetidas)
 - Permite detectar tramas perdidas
- **Códigos de redundancia → **puede corregir****
 - Se añaden una serie de bits obtenidos a partir de una operación sobre los datos (comprobar si el mensaje es correcto o no)
 - Permite detectar tramas corruptas e incluso corregir bits erróneos
- **Bit de paridad (para detectar el error, no corregir)**
 - Se añade un 1 si el número de 1s en el mensaje es par
 - Se añade un 0 si el número de 1s en el mensaje es impar
 - Trama: 011010 ->0110100 → **impar**
 - Si cambia un solo bit, el destino puede darse cuenta de que ha ocurrido un error

numera
y
comprueba

raíz cuadrada
y
comp. resultado

- Distancia de Hamming: Número de bits diferentes en dos palabras
- Algoritmos de detección
 - Suma de verificación: La suma de diferentes partes de la trama permite tener un campo que ayuda a corregir
 - Códigos de redundancia cíclica (CRC): Se calcula un polinomio que se divide por diferentes partes de la trama
- Algoritmos de corrección (nos ahorraremos el reenvío, muchos bits, desperdicio info)
 - Códigos de Hamming
 - Códigos de Reed-Solomon

5. Técnicas ARQ → ventana deslizante (control de flujo)

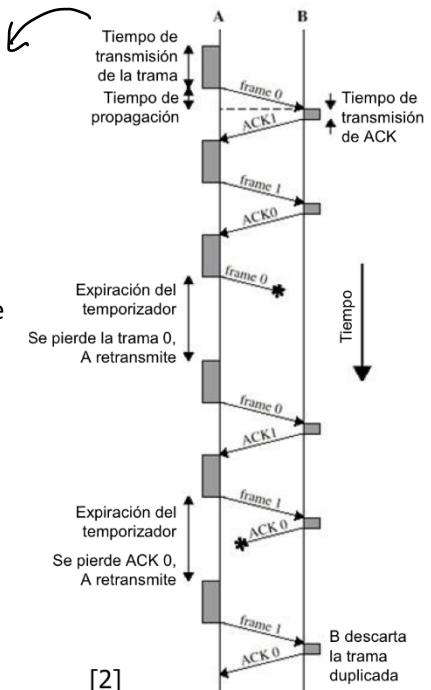
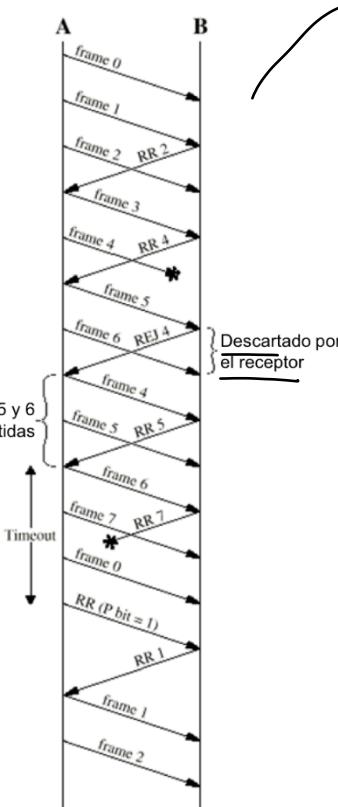
- Solicitud de repetición automática (Automatic Repeat reQuest)
 - Conjunto de un enlace que combinan distintos mecanismos de control de flujo y control de errores ↗ q.
 - Técnicas más comunes

▪ ARQ de parada y espera: Basado en la técnica de parada y espera estudiada previamente, se utilizan temporizadores para el reenvío de las tramas no asentidas, eliminación de duplicados.

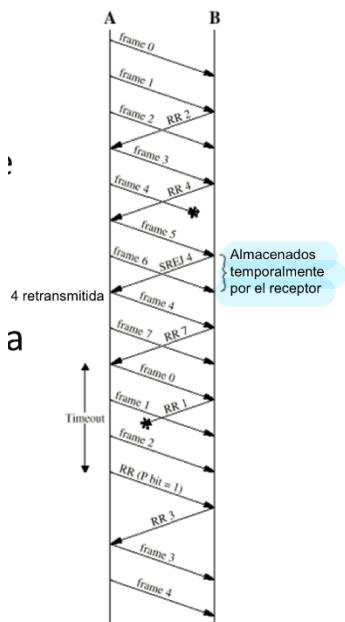
▪ ARQ de ventana deslizante con rechazo simple: Basado en el control de flujo mediante ventana deslizante, receptor solicita retransmisión de trama dañada o perdida, emisor repite trama solicitada y las que había enviado tras ella, eliminación de duplicados, las tramas fuera de orden se descartan, se puede solicitar el reenvío de confirmaciones

- Limitaciones en el tamaño de la ventana con ARQ con rechazo simple:
- Si se utilizan k bits para el número de secuencia, el tamaño máximo de la ventana es $2^k - 1$
- ¿Por qué?
- Supongamos que se utilizan números de secuencias de bits (0-7) y tamaño de ventana 8 $2^3 = 8$
- El emisor envía la trama 0 y recibe de vuelta un RR1
- A continuación, el emisor envía las tramas 1, 2, 3, 4, 5, 6, 7, 0 y recibe de vuelta un RR1
- ¿Qué significa?
- A) Las 8 tramas se han recibido y RR1 es un asentimiento acumulativo para todo el bloque de tramas
- B) Las 8 tramas se han deteriorado y se está repitiendo el RR1 anterior
- ARQ de ventana deslizante con rechazo selectivo: Basado en control de flujo mediante ventana deslizante, receptor solicita retransmisión trama dañada o perdida, emisor repite solo la trama solicitada, las tramas fuera de orden pueden almacenarse, se

zo
na
e
n



$$2^3 = 8$$



puede solicitar el reenvío de confirmaciones, eliminación de duplicados

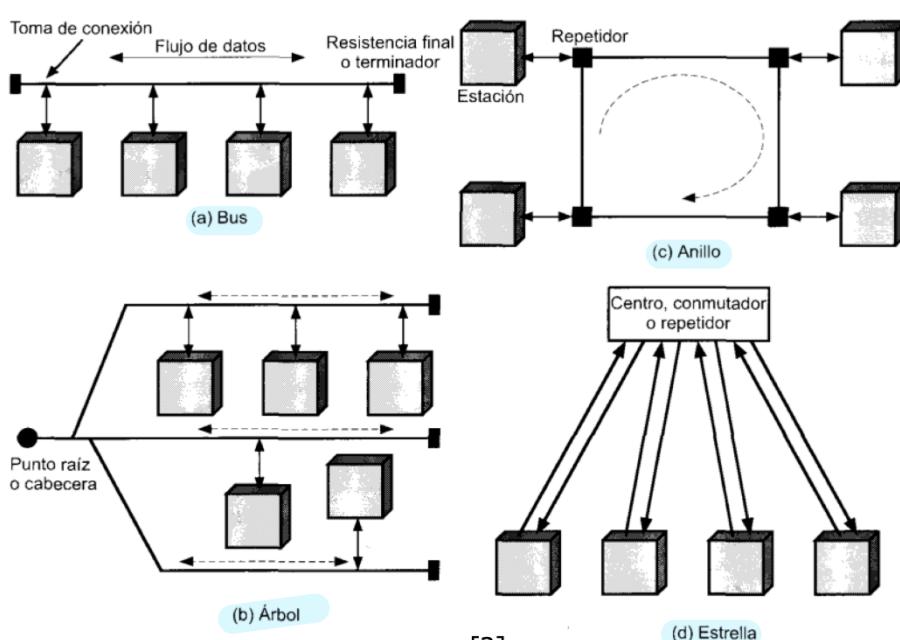
- Limitaciones en el tamaño de la ventana con ARQ rechazo selectivo:
- Si se utilizan k bits para el número de secuencia, el tamaño máximo de la ventana es 2^{k-1} $2^{8-1} = 4$
- ¿Por qué?
- Supongamos que se utilizan números de secuencia de 3 bits (0-7) y tamaño de ventana 7
- El emisor envía las tramas 0 a 6
- El receptor recibe correctamente las 7 tramas y envía un RR7
- RR7 se pierde
- El temporizador del emisor expira y retransmite todas las tramas
- El receptor esperaba las tramas 7, 0, 1, 2, 3, 4 y 5
- El receptor supone que la trama 7 se ha perdido y acepta las tramas 0 a 5 como tramas nuevas

6. Redes de área local

- Características

- Local Area Network (LAN)
- Medio de transmisión compartido por múltiples estaciones
- Cubren distancias relativamente reducidas
- Suelen tener unas tasas de transmisión bastante elevadas
- Tienen un bajo coste
- Usos principales
 - Redes de trabajo
 - Redes de respaldo y almacenamiento
 - Redes troncales

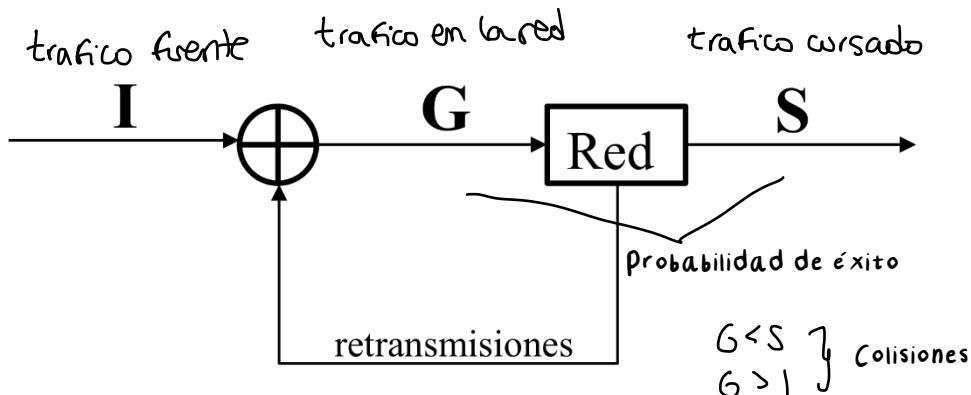
- Topologías



- Bus: Varios equipos conectados directamente a un mismo medio de transmisión lineal (Bus), las tramas transmitidas se propagan por todo el medio, todos los equipos comprueban la dirección para saber si la trama va dirigida a ellos, la señal es absorbida por los extremos del bus.
- Problemas Bus: Es complicado encontrar la potencia de señal adecuada, suficientemente alta para no ser sensible al ruido, no excesiva para evitar saturar el bus. La longitud de los buses es limitada, se pueden extender mediante el uso de repetidores
- Anillo: formada por un conjunto de repetidores unidireccionales unidos por enlaces punto a punto, todos los equipos comprueban el campo de dirección de la trama y lo copian si va dirigido a ellos. La estación de origen retira la trama cuando le vuelve
- Problemas anillo: Sincronización entre estaciones: Si ocurre un pequeño desfase, no se sabe como o cuando seguir retransmitiendo, el fallo de un único repetidor o enlace inutiliza la red, añadir una nueva estación al anillo implica parar el sistema
- Estrella: Cada estación está conectada a un nodo central, el nodo central puede difundir: Se retransmite la trama por todos los enlaces de salida; conmutar: La trama solo se retransmite por el enlace adecuado; Muy sensible ante fallos en el nodo central
- Hub (concentrador): Retransmite la señal a todas las salidas
- Switch (comutador): Retransmite la señal solo por la salida adecuada, utiliza una tabla de direccionamiento para conocer las MACs de los dispositivos, comutador lento: Comprueba el CRC de la trama, comutador rápido: Retransmite la trama en cuanto identifica la dirección de salida → MAC (trama)

7. Control de acceso al medio

- Utilización del medio compartido: Las estaciones transmiten de forma independiente, se utiliza un mismo medio de transmisión, cuando dos estaciones transmiten a la vez, se produce una colisión (es necesario retransmitir), la gestión se realiza en una subcapa conocida como MAC (Media Access Control), se busca optimizar el uso del canal sin saturarlo
- Clasificación técnicas MAC
 - Centralizadas: Una sola estación gestiona el acceso, lógica de acceso sencilla, no es necesario coordinarse entre estaciones → produce cuello de botella
 - Descentralizadas: Varias estaciones gestionan el acceso, mas robustas ante fallos, no se produce cuello de botella en la gestión → no producen cuello de botella
 - Síncronas: Se pre-asigna una capacidad para cada conexión, no adecuado para LANs, cantidad muy variable de elementos conectados y tráfico a ráfagas, se utilizan técnicas de multiplexación, casos de uso: emisión radio, televisión... ↳ capa física
 - Asíncronas o dinámicas: Se consigue en cada trama, la capacidad necesaria para ella
- Modelado del tráfico
 - Trafico fuente (I): tráfico que las máquinas intentan transmitir
 - Trafico cursado (S): tráfico que la red consigue entregar
 - Trafico en la red (G): Trafico que circula por la red



- En todos los casos $S=G \cdot$ Probabilidad éxito
 - Si no se producen colisiones $S=G=I$
 - Si se producen colisiones $S < G$; $I < G$; Si la red no está saturada $-I=S$; Si la red no está saturada $-S < I$
- $I \leq S \rightarrow$ no está saturada

- Tipos de técnicas asíncronas

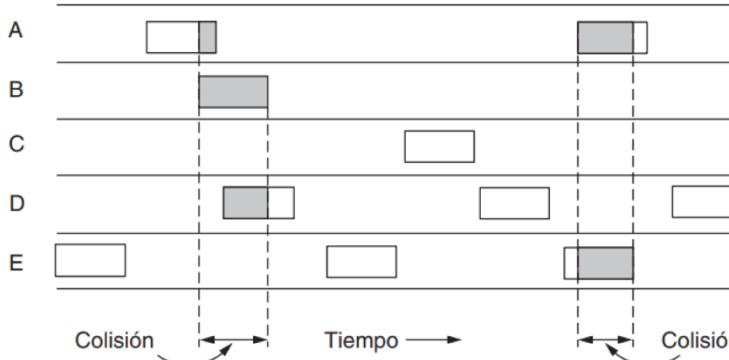
- Contienda: Las estaciones compiten por transmitir, gestión distribuida, bueno si la carga es baja y el tráfico a ráfagas \rightarrow poca carga
 - ○ Rotación: Las estaciones transmiten de acuerdo a una serie de turnos, pueden ser centralizada o distribuida, adecuado si hay muchas estaciones y mucha carga \rightarrow mucha carga
 - ○ Reserva: Las estaciones reservan parte de la capacidad del canal, puede ser centralizada o distribuida, bueno si hay pocas estaciones y mucha carga
- Técnicas de contienda:** cuando se tienen datos, las estaciones intentan transmitir, se tiene que escuchar el medio de transmisión, es posible que se produzcan colisiones, en caso de colisión es necesario: detectar la colisión, decidir cuando retransmitir
- ALOHA: Protocolo muy sencillo que transmite cuando se tienen datos, si hay colisión, espera un tiempo aleatorio y se vuelve a retransmitir, rendimiento con fuentes infinitas y llegadas exponenciales $S=G \cdot e^{-2G}$

muchas estaciones

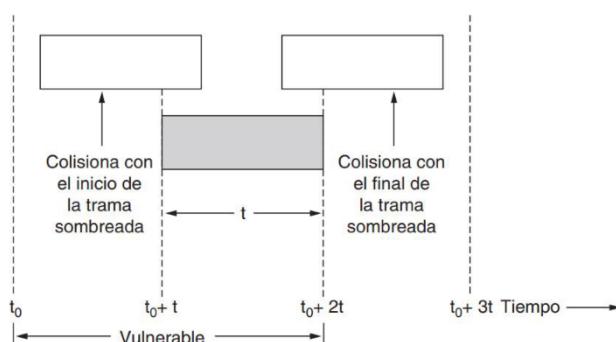
pocas estaciones

poca carga

Usuario

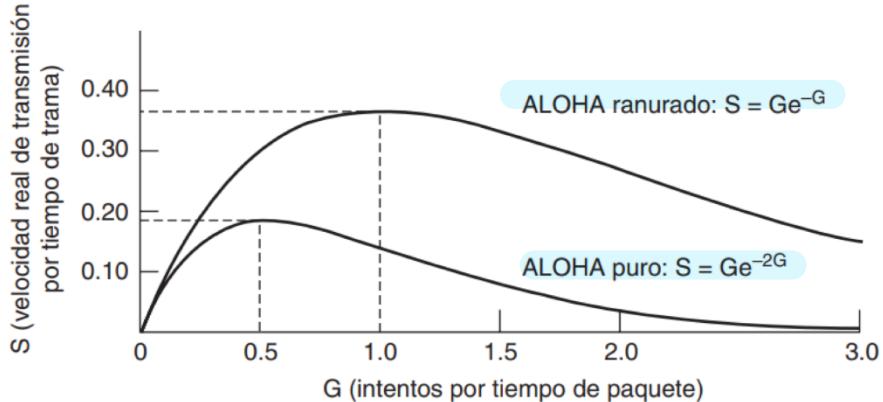


Para transmitir una trama con éxito, no se puede solapar nada con ninguna otra trama, si hay alguna otra trama en el canal, ambas se perderán, aunque coincidan mínimamente, con tramas de tamaño constante t , una trama es vulnerable durante $2t$



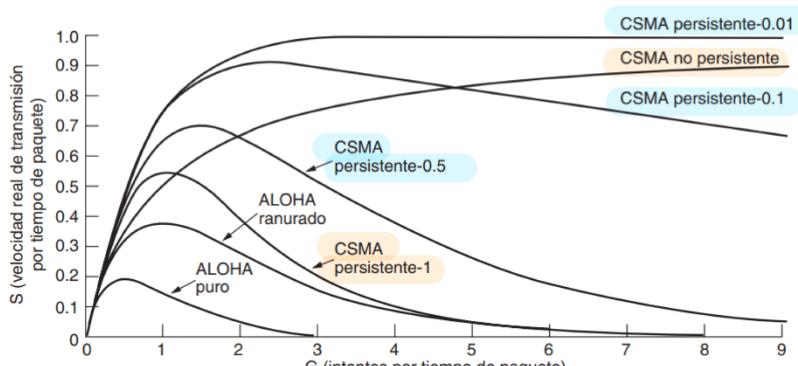
- ALOHA ranurado: El tiempo se divide en ranuras de tamaño t, las estaciones solo pueden comenzar a transmitir una trama al comienzo de la ranura, la probabilidad de colisión es menor, solo si hay otra transmisión en la misma ranura, rendimiento: $S = G \cdot e^{-G}$ ~~ya no está el 2~~
- ALOHA vs ALOHA ranurado: máximos
 - ALOHA: $G=0.5 \rightarrow S \approx 0.184$
 - ALOHA ranurado: $G=1 \rightarrow S \approx 0.368$

ranurado > ALOHA



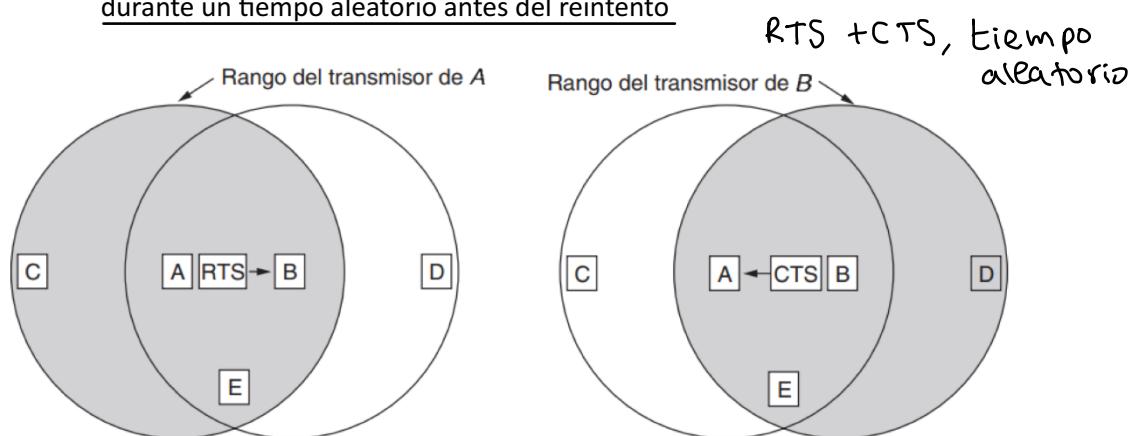
- CSMA: Acceso múltiple por detección de portadora (Carrier Sense Multiple Access), las estaciones están escuchando el medio de transmisión, esperan a que el canal esté libre para empezar a transmitir, motivos para las colisiones, dos estaciones empiezan a transmitir a la vez al acabar otra, debido al retardo de propagación
 - CSMA persistente-1: funcionamiento, las estaciones escuchan el medio, si está ocupado, esperan hasta que quede libre, si está vacío, transmiten, si hay colisión, se espera un tiempo aleatorio, se vuelve al primer paso. Problema, se suelen producir colisiones al final de los envíos de tramas
 - CSMA no persistente: funcionamiento, las estaciones escuchan el medio, si está ocupado, se espera un tiempo aleatorio, se vuelve al primer paso, si está vacío, transmiten, si hay colisión, se espera un tiempo aleatorio, se vuelve al primer paso. Problema, medio desaprovechado justo tras el fin de una transmisión
 - CSMA persistente-p: funcionamiento, las estaciones escuchan el medio, si está ocupado, esperan hasta que quede libre, si está vacío, transmiten con probabilidad p, se vuelve al primer paso con probabilidad (1-p), si hay colisión, se espera un tiempo aleatorio, se vuelve al primer paso. Se busca un equilibrio entre reducir el numero de colisiones y el tiempo de desocupación.

• Técnicas de contienda – rendimiento



→ CSMA con detección de colisión

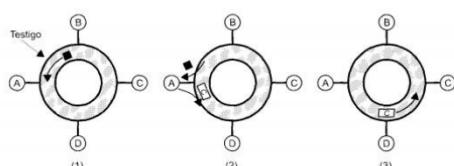
- CSMA/CD: problema común en técnicas CSMA, el medio permanece inutilizable durante el tiempo que dos tramas colisionan, técnica CSMA con detección de colisión (CD, Collision Detection), las estaciones escuchan mientras transmiten, si detectan colisión: Las estaciones escuchan mientras transmiten. Si detectan colisión: Transmiten una pequeña señal de interferencia. Abordan el envío
- MACA: Las técnicas CSMA no son adecuadas para redes inalámbricas. Es difícil detectar las colisiones, puede haber estaciones "ocultas". Acceso múltiple con evitación de la colisión (Multiple Access with Collision Avoidance): No se escucha el medio para detectar colisiones, evita colisiones entre estaciones que no se ven. Problemas: Las colisiones no son detectadas por la capa MAC, se reenvían cuando lo detectan las capas superiores, mucho tiempo después de la colisión.
Funcionamiento: Se utilizan RTS (Request to send) y CTS (Clear to send) para bloquear el medio. Si se produce colisión durante el envío, se espera durante un tiempo aleatorio antes del reintento



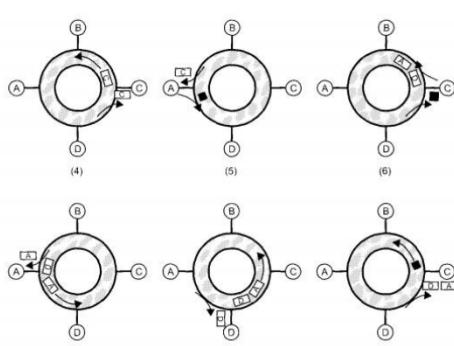
- Técnicas de rotación: Las maquinas transmiten en orden, no se producen colisiones. Técnicas basadas en sondeo (centralizadas) una estación controladora da el turno al resto de estaciones, las estaciones informan a la controladora al acabar. Técnicas basadas en el paso de testigo (distribuidas) existe una trama que hace de testigo, la estación que tiene el testigo puede transmitir, el testigo se pasa al acabar de transmitir o pasar un tiempo determinado

**muchas
estaciones,
muchísima
carga**

- Token ring: utiliza una topología en anillo, se basa en el uso de un testigo para efectuar la transmisión, una estación espera a tener el testigo para enviar sus tramas, cuando la trama pasa por la estación de destino, esta la copia y la mantiene en el anillo, una vez que las tramas vuelven a la estación de origen, esta libera el testigo y lo pone de nuevo en el anillo



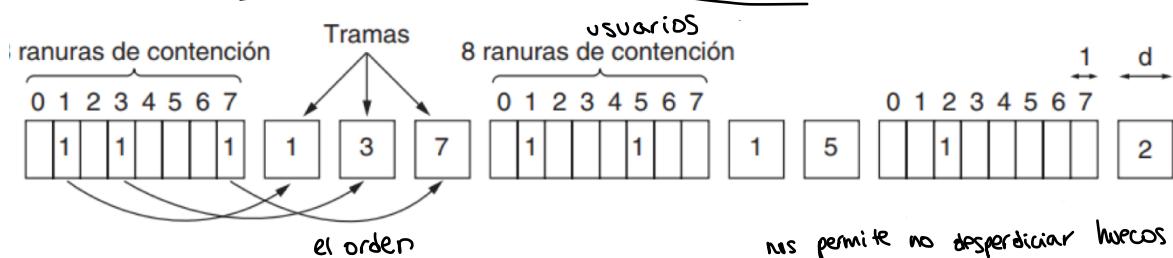
por orden



pocas estaciones, mucha carga

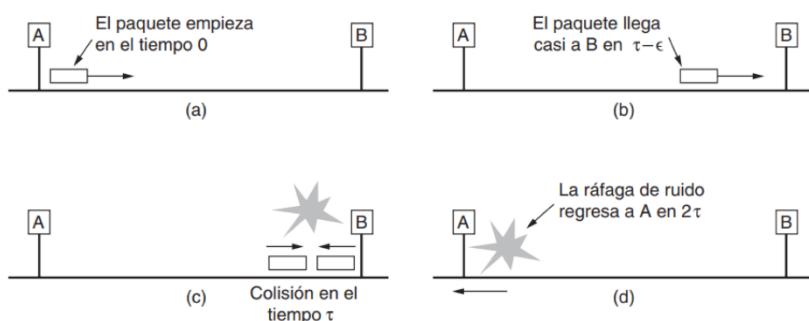
- Técnicas de reserva: El tiempo se divide en diferentes instantes: Periodos de contención, las estaciones indican que quieren transmitir. Periodos de transmisión, las estaciones transmiten los datos en los instantes que han reservado previamente. No se producen colisiones, ya que nos garantizamos que no se transmite a la vez

- o Mapa de bits (no hay una estación central, se disputan cual va con cual): el periodo de contención se divide en ranuras de reserva, cuando tiene datos para transmitir, rellena su ranura con un 1. En el periodo de transmisión, se espera tanto tiempo como tramas fueran reservadas, las tramas se transmiten en orden. Perfecto para personas, ya que generamos ráfagas a picos (usuarios), nos permite no desperdiciar huecos



8. El modelo de referencia IEEE 802 (intenta que todos los dispositivos se comuniquen correctamente)

- Se encargan de definir algunos de los estándares mas utilizados hoy en día
 - o 802.3 ethernet
 - Preámbulo: Siete veces seguidas la cadena 10101010. Permite la sincronización entre emisor y receptor
 - Star of frame o comienzo de trama: La última secuencia del preámbulo 10101011 para indicar que se inicia la trama.
 - Direcciones de origen y destino: Direcciones MAC de las máquinas que emiten y reciben
 - Longitud: tamaño del campo de datos LLC
 - Datos: información recibida de la capa LLC
 - Relleno: bytes añadidos por si la trama no tiene el tamaño mínimo para evitar colisiones
 - Suma de verificación: se utiliza para calcular el CRC y comprobar que no ha ocurrido ningún error en la transmisión, se utiliza todos los campos excepto el preámbulo y la propia suma de verificación
 - Tiempo mínimo necesario para que una estación que empieza a transmitir, se de cuenta de una colisión mientras está transmitiendo (2 veces el tiempo de propagación del canal)

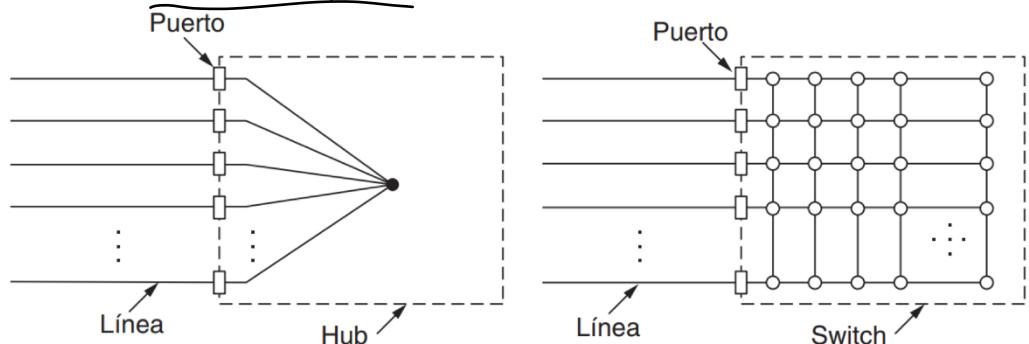


- CSMA/CD con retroceso exponencial binario: Sirve para determinar el tiempo de espera después de una colisión. Tras k colisiones, con $k \leq 10$, se espera $n \cdot t_{\text{prop}}$ con n elegido entre 0 y $2^k - 1$. Tras k colisiones, con $10 < k \leq 16$, se espera $n \cdot t_{\text{prop}}$ con n elegido entre 0 y 1023. Si hay mas de 16 colisiones, se desiste

- Direcciones MAC: cada tarjeta tiene asociada una dirección MAC, está compuesta por 48 bits representados en hexadecimal en grupos de 8, los tres primeros octetos identifican al fabricante, cada tarjeta tiene una dirección de red única. Ejemplo:
1a:2b:3c:4d:5e:60-1A2B.3C4D.5E.60 6 bloques
FF:FF:FF:FF:FF:FFFF.FFFF.FFFF ↳ 8 grupos → 48 bits

- Ethernet comutada: Originalmente se colocaba repetidores y concentradores para aumentar el tamaño de la red, conocidos como hubs. Aunque cada máquina estuviera conectada a un cable diferente, el hub repetiría la señal por todos los cables, por lo que realmente las estaciones estarían compartiendo el medio. Aparece una solución comutada, los switches, que repiten solo la trama por la salida correspondiente

hubs
o
switch



- Ethernet comutada (Switches): Son una solución más compleja y cara, aunque con el paso del tiempo se ha abaratado y hoy en día es la opción más utilizada. Los Switches permiten separar dominios de colisión, mejorando el rendimiento de la red. Poseen tablas en las que relacionan interfaces de salida con direcciones MAC. En el caso de enviarse una dirección de difusión, la retransmitiría por todas las salidas

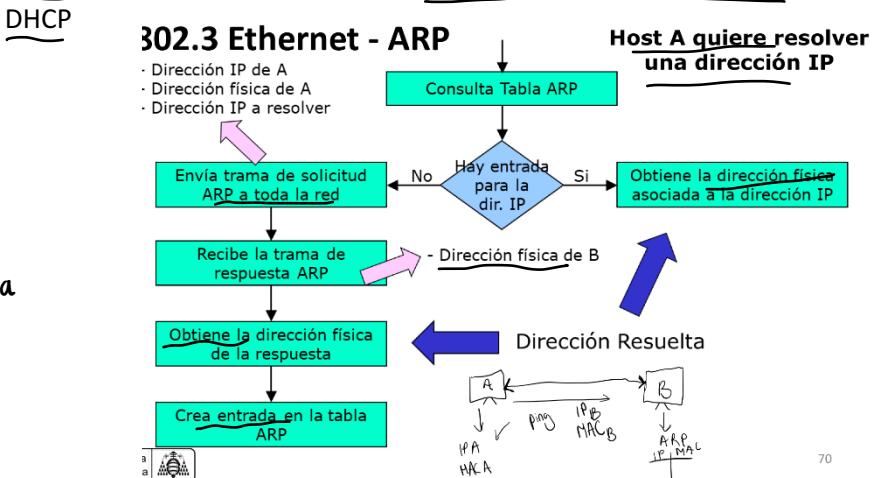
- Ethernet (ARP): Protocolo de resolución de direcciones (Address Resolution Protocol). Se encarga de obtener las direcciones MAC de las máquinas, a partir de una dirección IP. Es un protocolo que se implementa en equipos que también poseen nivel de red, almacenan unas tablas que relacionan MACs con IP. Su variante inversa es RARP (Reverse ARP), que asigna direcciones IP a partir de las MAC, hoy en día en desuso, principalmente sustituido por DHCP

resolución
de direcciones

ARP vs DHCP

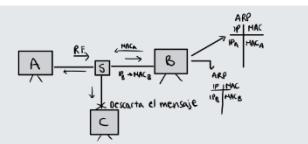
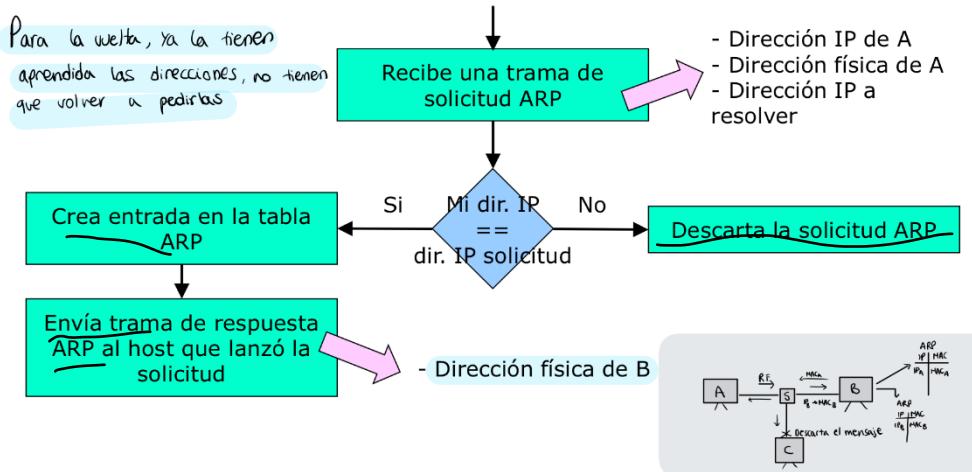


La que mas se usa



• 802.3 Ethernet - ARP

Host B recibe la trama de solicitud ARP de A

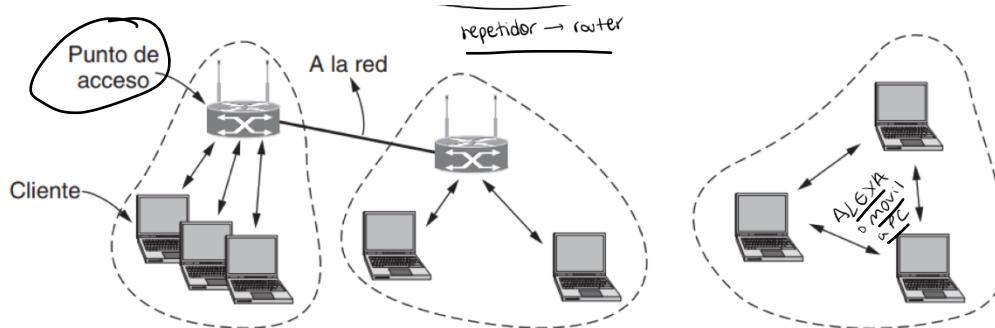


- Actualizaciones: (Par trenzado) Fast ethernet 802.3u: Aumenta la velocidad hasta 100 Mbps. Incluye autonegociación para facilitar retrocompatibilidad; Gigabit Ethernet 802.3ab: Alcanza 1Gbps, extensión de portadora y ráfagas de trama para ampliar el rango de alcance de la red; (fibra óptica) Gigabit ethernet y terabit ethernet: mejoras sucesivas que amplían la velocidad y el alcance de las redes de tipo ethernet

○ 802.11 wifi (2.4-5 GHz)

- Define un estándar de comunicaciones inalámbrico de corto alcance. Es necesario utilizar bandas del espectro electromagnético que estén libres. Requiere diferentes técnicas de acceso al medio que Ethernet u otros estándares cableados. Al igual que otros estándares 802, divide el nivel de enlace en dos subcapas, buscando aíslar al nivel de red
- Puede utilizarse para conectarse a la red de Internet, o para crear una red local, elemento clave: punto de acceso (Access Point AP)

11 WiFi



▪ Servicios:

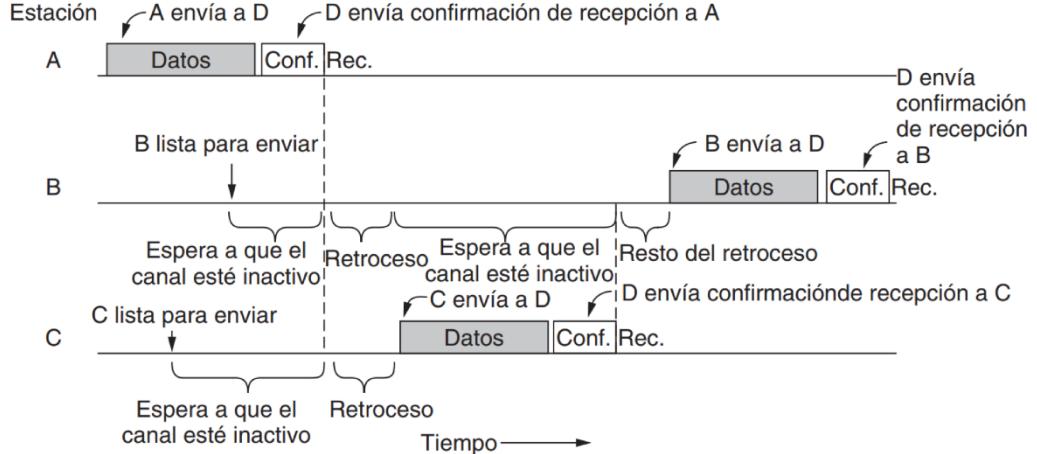
- conectarse → Asociación: permite a una estación, conectarse a un AP u otra estación
- desconectarse → Desociación: Permite que una estación notifique su intención de abandonar una celda
- Cambio → Reasociación: cambiar de un AP a otro sin necesidad de desasociarse
- Autenticación: Identificar a una estación para saber si puede o no conectarse a la red (WEB Wired Equivalent Privacy comprobar que la persona que se conecta, es la

wifi cifrado, ethernet, no

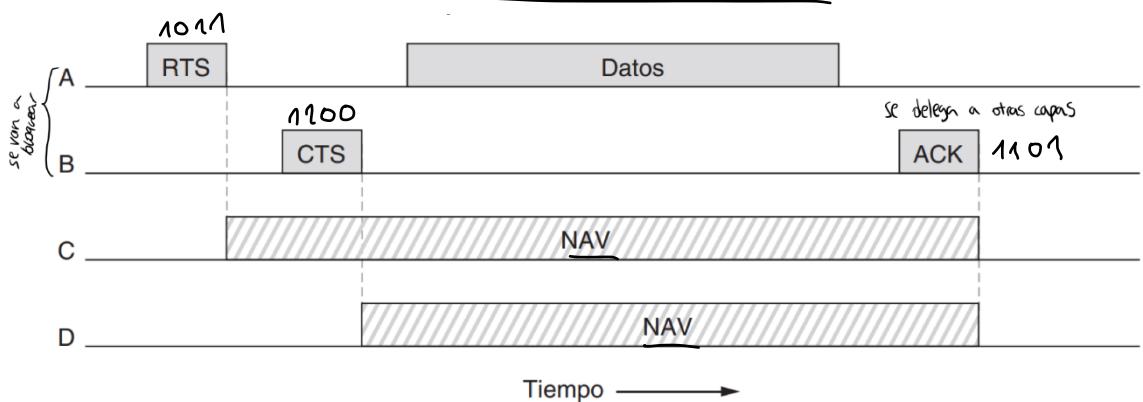
que es, van cifradas las comunicaciones en wifi, en ethernet NO), WPA WiFi Protected Access (combinadas con encriptación, WPA1 muy fácil desencriptar, WPA2 muy complicado desencriptar, WPA3 no se puede desencriptar))

- Capa física: utiliza los elementos de 2.4Ghz (mayor alcance, 11 canales) y 5Ghz (mas velocidad), ha evolucionado utilizando canales con anchos de banda desde 20 hasta 160 Mhz, multiple input – multiple output (MIMO) (varios canales en un punto de acceso (antenas, router gaming)). Multiplexación por división de frecuencias ortogonales (OFDM – orthogonal frequency – division multiplexing). Mejoras en la eficiencia y el alcance, usando también en redes de telefonía móvil
- Capa acceso al medio: No se puede escuchar y transmitir a la vez, señal de llegada mucho más débil que transmitida. CSMA/CA – CSMA con evitación de colisiones (Collision Avoidance), cuando se tiene una trama para transmitir, se escucha el medio y si se está libre, transmite. Si esta ocupado, se espera a que se acabe y se espera un tiempo aleatorio para transmitir. Si durante la espera fin, aleatoria, alguien transmite, el tiempo de espero se "pausa". Se utilizan confirmaciones de recepción.

El procedimiento de enviar un mensaje



CSMA/CA se complementa con NAV (Network Allocation Vector)
Permite evitar el problema de las estaciones ocultas



NAV → evita problema
estaciones ocultas

- Formato de trama

destino fuera de la red local

Bytes	2	2	6	6	6	2	0-2312	4			
	Control de trama	Duración	Dirección 1 (receptor)	Dirección 2 (transmisor)	Dirección 3	Secuencia	Datos	Secuencia de verificación			
las direcciones son de 6 bits											
[1]											
datos											
Bits	2	2	4	1	1	1	1	1			
	Versión = 00	Tipo = 10	Subtipo = 0000	Para DS	De DS	Más frag.	Rein-tentar	Admón. energía	Más datos	Protegida	Orden

- Versión: Actualmente 00, pero podría cambiar en el futuro
- Tipo: Gestión (00), control (01) o datos (10)
- Subtipos: RTS (1011), CTS (1100), ACK (1101) ...
- Para/De DS: Define si el envío es entre estaciones de una misma red, entre estación y AP o entre APs
- Más fragmentos: Indica si la trama se ha partido para enviarse por el medio
- Reintentar: especificar si la trama es un reenvío
- Admon Energía: Utilizado por el emisor para indicar que va a entrar en modo de ahorro de energía
- Protegida: Especifica si la trama fue cifrada
- Orden: Indica al receptor que la capa superior espera que la secuencia llegue en riguroso orden
- Duración: tiempo de espera de las demás estaciones antes de comprobar el canal (NAV)
- Direcciones: origen y destino en la red local. La tercera dirección es el destino fuera de la red local
- Secuencia: Numera las tramas para detectar duplicados
- Datos: información pasada por la capa superior
- Suma de verificación: Comprobación que la trama llegó correctamente

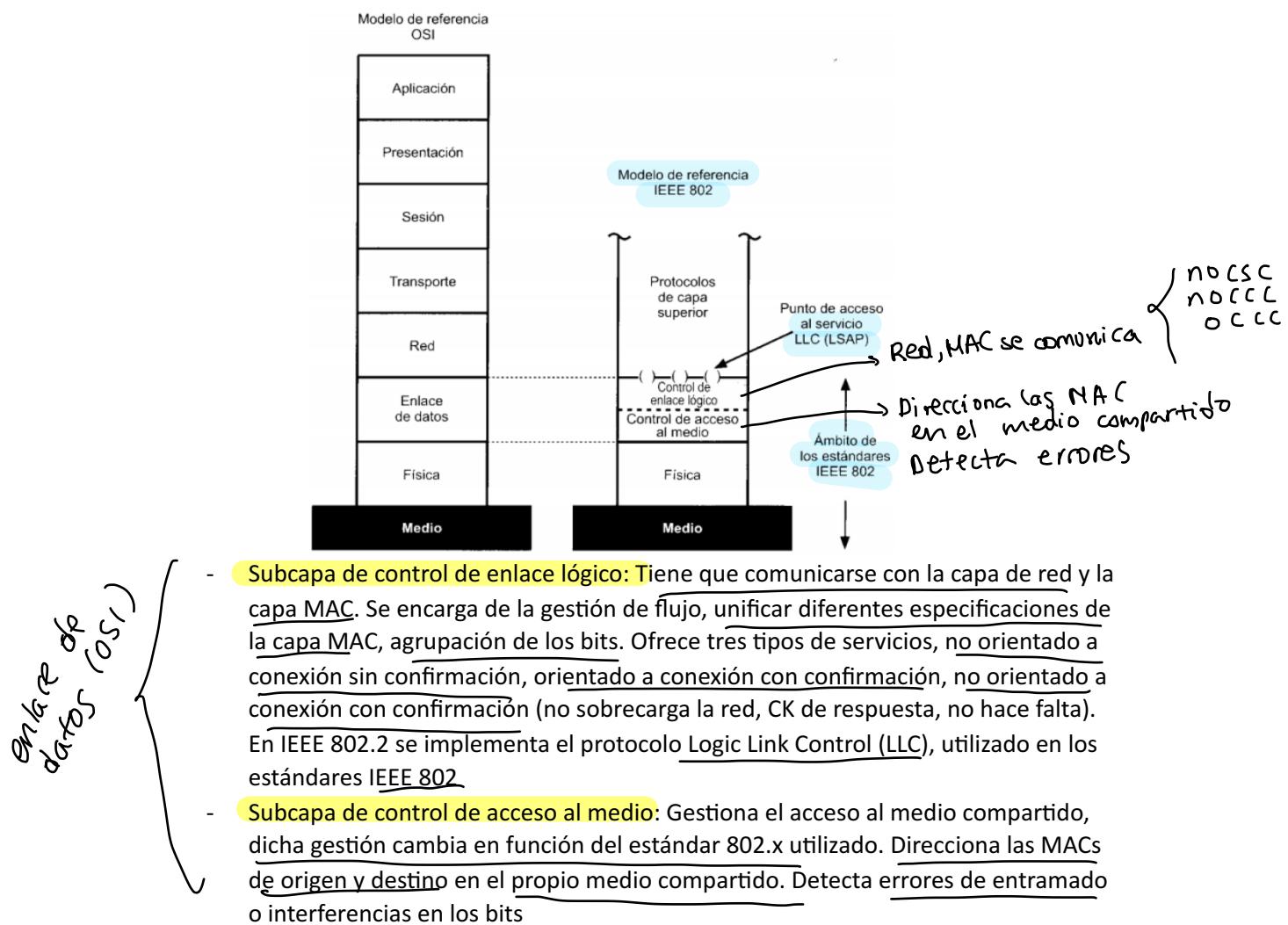
Control de trama

PAN → IS
WiMAX → 16

- 802.15 WPAN (bluetooth, zigbee)
- 802.16 WiMax (zonas rurales)

- Se utiliza sobre todo en los niveles mas bajos del modelo OSI

- **Modelo de referencia**



Tema 4: Nivel de red → Internet, datagrama (IP)

↓ sin comunicación previa

1. Introducción

- **Encaminamiento de paquetes desde el origen hasta el destino (se encarga nodo a nodo por donde se envía)**
 - Proporciona una interfaz de red al nivel de transporte
 - No se encarga únicamente de la conexión extremo a extremo
 - Gestiona los pasos a través de los diferentes nodos intermedios
 - Una de sus funciones es buscar la ruta mas apropiada
 - Utiliza tablas de encaminamiento (el gps de internet) → tablas encaminamiento ↴ mapa
 - Almacena información sobre los destinos conocidos
 - Indica cual es el siguiente nodo al que enviar la información para seguir con la ruta
- **Control de la congestión (evitar enviar tráfico por líneas saturadas)**
 - Evitar la sobrecarga de las líneas → capa transporte (segmento)
 - Tarea compartida con el nivel de transporte (de extremo a extremo) (puerto)
 - Control a lo largo de la red, no solo entre extremos
- **Calidad de servicio (QoS)**

- Ancho de banda
- Retardo y variación del retardo
- Perdida

Parametros para determinar la calidad

2. Protocolo IP

no se sabe si llega la info.

- Características

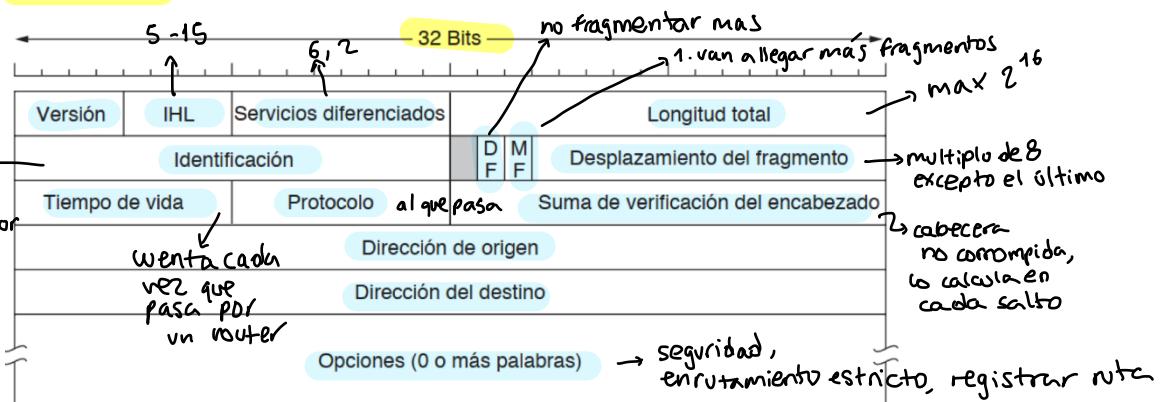
- No orientado a conexión: cada datagrama se trata de forma independiente, pudiendo seguir caminos distintos
- No fiable: (no se sabe si los mensajes llegan correctamente) es decir, cuando se produzca algún error los datagramas se perderán
- Inseguro: la entrega de los datagramas no está garantizada: se pueden perder, duplicar, retrasar o entregarse fuera de orden (poco esfuerzo)
- No incluye técnicas para la gestión de errores
- La unidad básica de información se denomina datagrama IP ¿IP es fiable o seguro? NO

- Funciones más importantes

- MAC de manera física -> no se cambia
- IP -> si se puede cambiar
- IPs que se repiten: 127.0.0.1, 192.198.X.X (IPs de routers, portátiles...)
- Direccionamiento: identificar a las máquinas mediante direcciones lógicas -> direcciones IP
- Encaminamiento: analiza los datagramas para encaminarlos por los nodos intermedios desde el origen hasta el destino
- Fragmentación y reensamblado: (mejoras ya que se reparte la información, mejor perder 0.01seg a perder 1seg) partición de los datagramas demasiado grandes para poder retransmitirlos por la red

MAC no mod.
IP si mod.

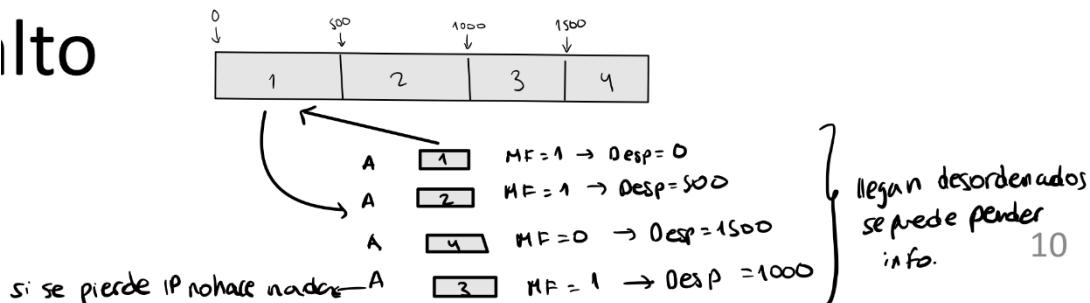
- Cabecera IP



- Versión: (6, es la que está esperando y no llega) indica la versión del protocolo a la que pertenece el datagrama
- Internet Header Length (IHL): tamaño total de la cabecera en palabras de 8 bytes. El tamaño mínimo es 5 y el máximo 15
- Servicios diferenciados: sirve para distinguir entre distintos tipos de servicios. Los 6 primeros bits indican la clase de servicio y los 2 restantes llevan información sobre congestión
- Longitud total: tamaño total del datagrama incluida la cabecera. El máximo son 2^{16} bits

- Identificación: identifica el fragmento de un paquete recién llegado. Todos los fragmentos de un paquete tienen el mismo identificador (pertener al mismo mensaje → juntarlos y tener el mensaje completo)
- Don't Fragment (DF): (no puede ser partido de nuevo: busca ruta alternativa, no lo envía) bit utilizado para comunicar al enrutador que no fragmente el paquete. Se puede utilizar para descubrir el tamaño máximo posible en una ruta concreta
- More Fragments (MF): (van a llegar más fragmentos de los esperados, cuando llegue el último se recomponen los fragmentos) indica que van a llegar mas fragmentos de un mismo datagrama. Salvo el último, todos los fragmentos tienen este bit a 1
- Desplazamiento del fragmento: indica a que parte del paquete pertenece el fragmento. Los fragmentos excepto el último deben ser múltiplos de 8 bytes
- Tiempo de vida (TtL): (cuenta cada vez que pasa por un router 128 o 256) contador para limitar el tiempo de vida de un paquete
- Protocolo: código que indica cual es el protocolo de la capa superior al que pasar el paquete
- Suma de verificación: asegura que la cabecera no ha llegado corrompida por el camino. Es necesario recalcular en cada salto

Ilto

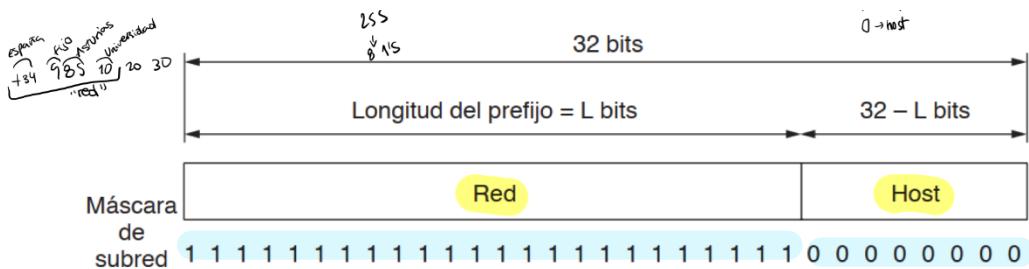


10

- Dirección de origen y destino: (MAC-> van cambiando, salto a salto) contienen las direcciones IP de las interfaces de red de origen y destino
- Opciones: permite añadir nuevas características no incluidas en la cabecera original
 - Seguridad: evitar enrutar paquetes a través de ciertas redes
 - Enrutamiento estricto: indicar todos los saltos desde el origen al destino
 - Registrar ruta: almacenar las IPs de todos los saltos realizados

- Direccionamiento IP (entra seguro en el examen!)

- Todas las máquinas conectadas a internet poseen una dirección IP de 32 bits que actúa como identificador
- Los 32 bits se dividen en 4 grupos de 8 bits separados por puntos
- Cada grupo se representa con notación decimal 156.35.14.2
- Toda dirección está compuesta de dos partes: una parte identifica la red y otra identifica al host
- Para saber que parte de la dirección corresponde a la red, utilizaremos una máscara de red
- La máscara se indica después de la dirección IP con un número entero que corresponde al número de 1s de la máscara 156.35.14.2/16 → 0/32 (16 1s y 16 0s en la máscara), 255→ 8 1s, IP junto una máscara, 1 → red, 0 → host



- Tipos de direcciones

- Unicast (unidifusión): dirección que identifica a un interfaz de red de una máquina (1 equipo).
- Multicast (multidifusión): dirección que identifica a un grupo de interfaces de red en distintas máquinas, nunca aparecerá como dirección de origen (mucho no a todos, en 1 red un grupo de equipos)
- Broadcast (difusión): dirección que identifica a todas las interfaces de una determinada red, nunca aparecerá como dirección origen (a todos, hace referencia a todos los equipos de la red)
- Públicas: direcciones visibles en Internet
- Privadas: direcciones que no son visibles en Internet (192.168.X.X redes locales, router-dispositivo)
- Estáticas: direcciones que no cambian en cada conexión (se asigna a alguien, hay que pagar)
- Dinámicas: direcciones que pueden cambiar en cada conexión (router -> internet, IP pública va cambiando)

	32 Bits			Rango de direcciones de hosts
Clase				
A	0	Red	Host	1.0.0.0 a 127.255.255.255
B	10	Red	Host	128.0.0.0 a 191.255.255.255 <small>2^16 equipos que redireccionar</small>
C	110	Red	Host	192.0.0.0 a 223.255.255.255 <small>2^24 equipos</small>
D	1110	Dirección de multidifusión		224.0.0.0 a 239.255.255.255 <small>último número, clase A,B,C ...</small>
E	1111	Reservada para uso futuro		240.0.0.0 a 255.255.255.255

como se diferencian

- Clase A – Máscara 255.0.0.0

- Direcciones privadas: 10.0.0.0 a 10.255.255.255
- Direcciones privadas: 127.0.0.0 a 127.255.255.255

- Clase B – Máscara 255.255.0.0

- Direcciones privadas: 127.16.0.0 a 127.31.255.255

- Clase C – Máscara 255.255.255.0

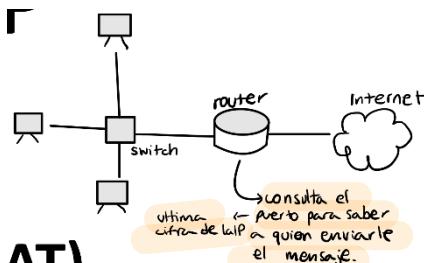
- Direcciones privadas 192.168.0.0 a 192.168.255.255

- Dirección base de red: dirección que identifica a la red

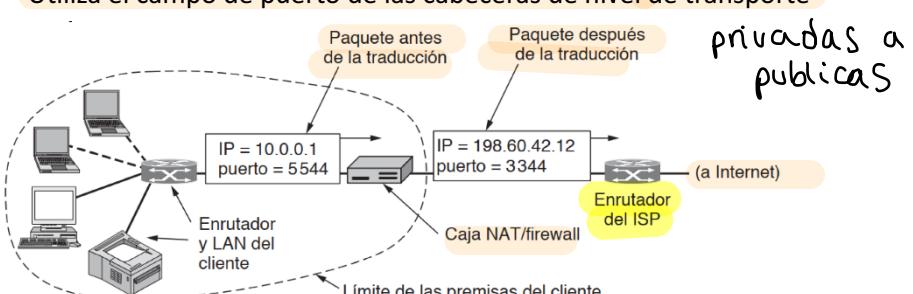
- Tiene todos los bits de la parte de host a 0

- Se obtiene realizando un AND bit a bit entre la dirección IP y de la máscara de subred
- Dirección de broadcast (identificar todos los elementos de la red, la máscara nos dice si es red, broadcast...)
 - Tiene todos los bits de la parte de host a 1 (255)
 - Se obtiene realizando un OR bit a bit entre la dirección IP y el complemento a 1 de la máscara
- El resto de direcciones libres se pueden asignar a los diferentes hosts libres
- Direcciones libres para n bits $\rightarrow 2^n - 2$
- Ejemplo 1 (2.5 puntos ejercicios de subred)
 - ID de red 156.35.0.0 \rightarrow clase B
 - Unas sola red, con espacio para $2^{16} - 2$ hosts
 - ¿Y si se quiere tener tres subredes?
 - Se puede dividir la red anterior en subredes más pequeñas
 - Se utilizarán parte de los bits de host para identificar las nuevas subredes
 - El tamaño de la máscara puede ser variable y dependerá del tamaño que se le quiera dar a la red – Variable Length Subnet Mask (VLSM)
 - ID de red 156.35.0.0 – Máscara 255.255.0.0
 - ID red \rightarrow 10011100 00100011 00000000 00000000
 - Mask \rightarrow 11111111 11111111 00000000 00000000
 - Para crear k subredes se necesitan n bits, que cumplan la ecuación $2^n \geq k \rightarrow$ se necesitan 2 bits
 - Mask \rightarrow 11111111 11111111 11000000 00000000
 - Habrá que hacer combinaciones con el 17º y 18º bit para generar los nuevos ID de cada subred
 - Mask \rightarrow 11111111 11111111 11000000 00000000
 - ID red 1 \rightarrow 10011100 00100011 00000000 00000000
 - ID red 2 \rightarrow 10011100 00100011 01000000 00000000
 - ID red 3 \rightarrow 10011100 00100011 10000000 00000000
 - ¿Y la combinación 11?
 - ¿Cuántos equipos entran en cada subred? ¿Sobrarán IPs?
- Ejemplo 2 (2.5 puntos ejercicios de subred) 00000000 \rightarrow No 100 equipos
 - ID de red 192.168.1.0/24 (tipo host)
 - Tres subredes, una con 100 equipos y las otras dos con 40
 - Solución: Utilizar dos bits de la parte de host para crear tres nuevas subredes
 - ¿Cuántos equipos entran en cada subred?
 - 6 bits libres para direccionar hosts
 - $2^6 - 2 = 62$ direcciones posibles
 - No se puede dividir utilizando máscara de tamaño fijo \rightarrow Hay que utilizar máscaras de tamaño variable (VLSM)
 - Número n de bits que se necesita para direccionar los k hosts de cada subred:
 - $2^n - 2 \geq 100 \rightarrow n=7$ (bits a cero de la máscara)
 - $2^n - 2 \geq 40 \rightarrow n=6$

- Cada una de las nuevas subredes tendrá una máscara que se adapte al número de bits que se necesitan para la parte de host
 - Subred 100 PCs -> Máscara de $32-7=25$ bits
 - Subredes de 40 PCs -> Máscara de $32-6=26$ bits
- ¿Cuáles serán los nuevos IDs de las subredes?
- Hay que dividir el ID original en redes más pequeñas:
 - Máscara 24 bits (original)
 - ID: 11000000 10101000 00000001 00000000
 - Máscara 25 bits
 - ID subred 1: 11000000 10101000 00000001 00000000
 - ID libres: 11000000 10101000 00000001 10000000 (la siguiente combinación disponible)
 - Máscara 26 bits (sumamos 1, pasamos al siguiente)
 - ID subred 2: 11000000 10101000 00000001 10000000
 - ID subred 1: 11000000 10101000 00000001 11000000 (la siguiente combinación disponible)
- Obtención de direcciones
 - Métodos
 - Configuración manual
 - Protocolo de autoconfiguración -> DHCP (dirección IP de manera automática)
 - Parámetros necesarios para configurar una máquina
 - Dirección IP
 - Máscara de red
 - Dirección IP del router de salida (si no está en la misma red el otro dispositivo) → página web
 - Dirección IP de servidores DNS (servidores de nombres, nombre página -> IP página)
 - Puerta enlace dispositivos -> IP router
- Protocolo DHCP (todo de manera automática, rellena los 4 parámetros necesarios)
 - Protocolo para obtener parámetros de configuración automática desde la red (por ejemplo, dirección IP)
 - Basado en el modelo cliente-servidor
 - El cliente contacta con un servidor DHCP para obtener sus parámetros
 - Asignación de dirección IP
 - Apropiada a la red o subred a la que se conecta el cliente
 - No asignada a otra máquina
- Network Address Translation (NAT) (IPv4)
 - Gestiona la posible escasez de direcciones IP (para repartir las IPs entre todos) dentro de una subred
 - Utiliza el campo de puerto de las cabeceras de nivel de transporte



última
cifra de IP
consulta el
puerto para saber
a quien enviarle
el mensaje.

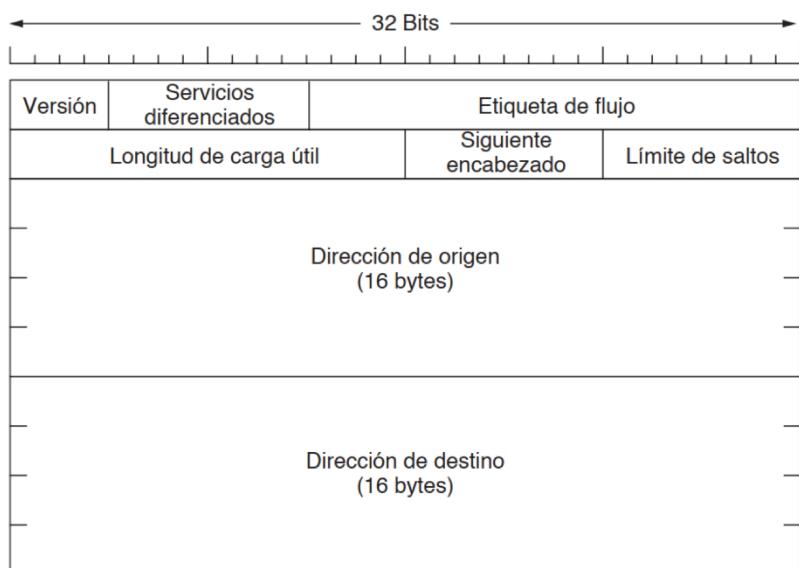


- IPv6 → 8
 - Implementa mejoras sustanciales sobre IPv4
 - Aumenta de forma notable la cantidad de direcciones existente en Internet 2^{32} vs 2^{128}
 - Es compatible hacia atrás, pero IPv4 (no compatible con IPv6) no es plenamente compatible con él.
 - No muy ampliamente extendido (30% dispositivos son compatibles con IPv6), pese a que fue desarrollado hace aproximadamente 20 años
 - Utiliza direcciones agrupadas en 8 bytes y escritas en hexadecimal:
 - 8000::::0123:4567:89AB:CDEF (Dirección más larga, :: para emitir una sucesión de 0s)

MAC → 6

IPv4 → 4

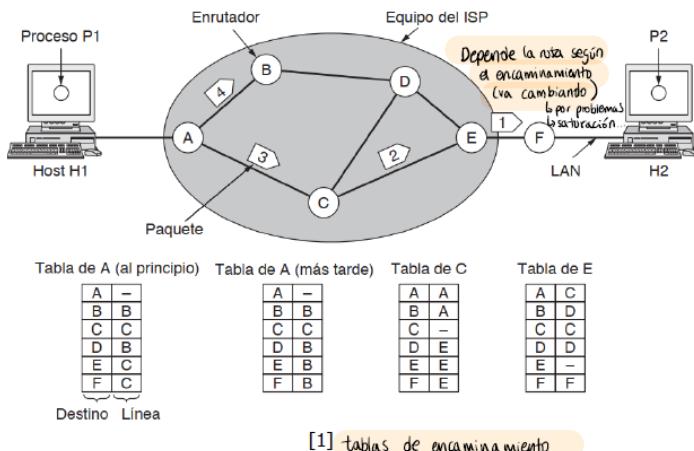
- IHL
- longitud total
- identificador
- DF, MF
- Desplazamiento del fragmento
- Tiempo vida
- Protocolo
- Suma verificación



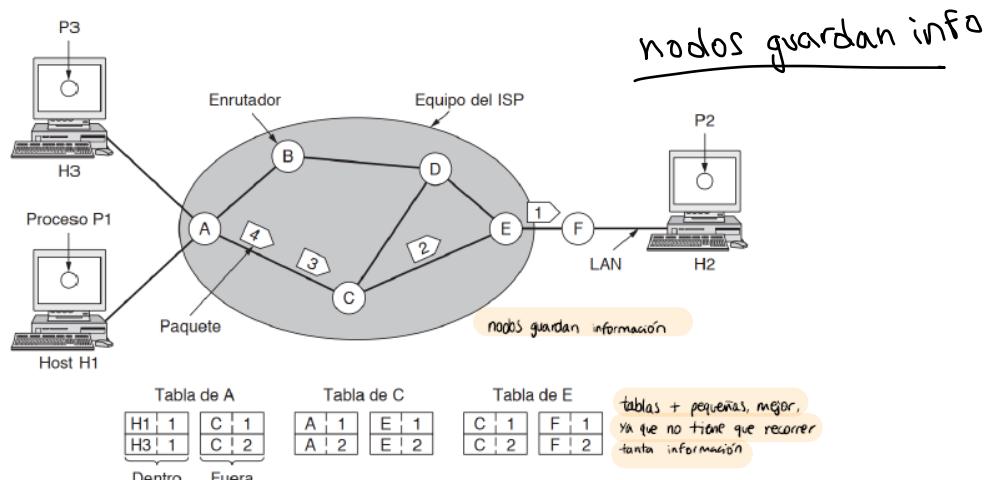
- Segmentación y reensamblado: Se dividen los paquetes varias veces tras el transcurso de envío. Se juntan todos los paquetes (reensamblado), se pueden perder paquetes o lleguen fuera de orden
 - ¿Dónde reensamblar?
 - En el destino: Los fragmentos solo se pueden hacer más pequeños
 - En los nodos intermedios: Uso de un gran espacio de almacenamiento, todos los fragmentos de los datagramas deben pasar a través del mismo dispositivo de encaminamiento
 - En IP se reensambla en el destino
 - Fallos en el reensamblado
 - Si se pierden paquetes, se descarta el reensamblaje
 - ¿Cuánto tiempo es necesario esperar para reensamblar?
 - Tiempo de vida para el reensamblado: asignar un tiempo al recibir el primer segmento. Si el tiempo expira sin completar el reensamblaje se descarta
 - Tiempo de vida del datagrama: si expira el tiempo de vida de un fragmento, se descarta el reensamblaje

3. Redes de datagramas y circuitos virtuales

- **Redes de datagramas:** Proporcionan un servicio de red no orientada a conexión, cada paquete puede seguir una ruta distinta a lo largo de la red (ej: Google maps - > de una ruta (varía según el tráfico), paquetes a rutas menos cargadas a más cargadas)
 - No se determina una ruta anticipadamente, cada datagrama se encamina independientemente con la que puede seguir rutas diferentes, los nodos mantienen una tabla de encaminamiento con las redes conocidas para encaminar los paquetes en función de su red de destino. El datagrama deberá contener la dirección completa del destinatario y del origen



- **Redes de circuitos virtuales:** Proporcionan un servicio de red orientado a conexión, los paquetes siguen el mismo circuito virtual a lo largo de toda la red
 - Establecen una ruta predeterminada al inicio de la conexión – Se tienen una ruta det. almacenan los siguientes nodos en una tabla. Los nodos no necesitan calcular la ruta cada vez que llega un paquete, ya la tienen almacenada. Todos los paquetes circulan por la misma ruta. Una vez que se termina la conexión, se liberan los recursos



virtuales

tiene que consultar las tablas siempre

cada 1 nodo, se caen todas las rutas que terminan en cuenta ese nodo

Asunto	Red de datagramas	Red de circuitos virtuales
Configuración del circuito	No necesaria	Requerida
Direccionamiento	Cada paquete contiene la dirección de origen y de destino completas	Cada paquete contiene un número de CV corto
Información de estado	Los enrutadores no contienen información de estado sobre las conexiones	Cada CV requiere espacio de tabla del enrutador por cada conexión
Enrutamiento	Cada paquete se enruta de manera independiente → <i>consultas tablas siempre</i>	La ruta se elige cuando se establece el CV; todos los paquetes siguen esa ruta
Efecto de fallas del enrutador	Ninguno, excepto para paquetes perdidos durante una caída	Terminan todos los CVs que pasaron por el enrutador defectuoso
Calidad del servicio	Difícil	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV
Control de congestión	Difícil	Fácil si se pueden asignar suficientes recursos por adelantado para cada CV

- Ventajas datagramas

- No consume recursos en el establecimiento de la conexión
- Mas fácil encontrar rutas nuevas
- Tiempo nulo de establecimiento de conexión
- Robustez ante caídas en la red
- Mas difícil de interceptar los mensajes completos (saber por dónde va a pasar)
- No necesita almacenar la información sobre múltiples circuitos virtuales

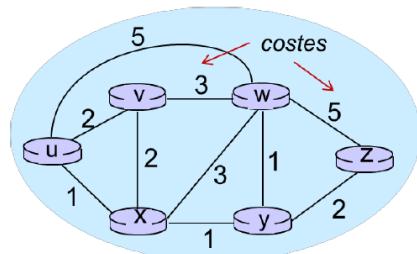
- Ventajas circuitos virtuales:

- No se genera sobrecarga por el cálculo de las rutas en cada nodo
- Paquetes mas ligeros al no utilizar direcciones completas
- Mayor facilidad para proporcionar un servicio fiable y con buena calidad

4. Algoritmos de encaminamiento (tipos genéricos en Ingeniería de redes -> se especifica)

- Encaminamiento: Encontrar la ruta óptima para interconectar diferentes redes
- Los diferentes nodos toman decisiones basándose en su conocimiento de la red
 - información de nodos vecinos
 - Conocimiento a priori de la topología
- Se utilizan protocolos de encaminamiento para obtener la mejor ruta posible
 - Estáticos
 - Dinámicos
- Encaminamiento estático (no hay un algoritmo ejecutándose en 2º plano)
 - Se configuran las rutas de forma permanente para cada par de nodos origen-destino
 - Las rutas son fijas
 - Solo cambiar cuando hay un cambio de topología
 - Los costes de enlace no pueden estar basados en datos dinámicos, pero pueden estar basados en volúmenes estimados de tráfico o en la capacidad de cada enlace

estimaciones
fijas

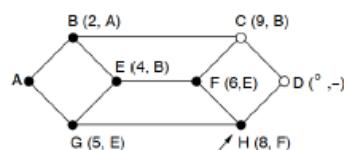
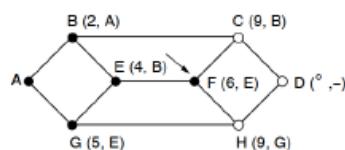
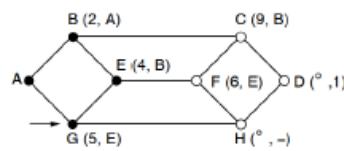
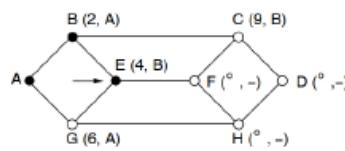
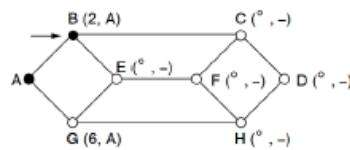
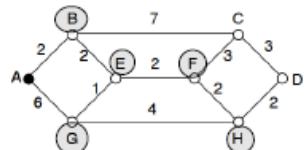


- Ventajas (para redes pequeñas): Carga de procesamiento mínima, fácil de configurar
 - Desventajas (para empresa pequeña fácil, para internet imposible): Configuración y mantenimiento prolongados y laboriosos, configuración propensa a errores (si hay muchos routers). Se requiere la intervención de un administrador para el mantenimiento de las tablas de rutas. No se adapta bien a las redes en crecimiento. Requiere un conocimiento completo de la red
 - Encaminamiento dinámico
 - Las rutas pueden cambiar para adaptarse a las variaciones de las condiciones en el conjunto de redes (se adapta el solo al añadir un router)
 - Principales condiciones que afectan a las decisiones de encaminamiento
 - Fallo de un encaminador: no se utilizará como parte de la ruta
 - Congestión: encaminar evitando la zona congestionada
 - Añadir nuevos nodos: comprobar si los nuevos nodos permiten rutas mas optimas que las existentes
 - Ventajas:
 - No es necesario reconfigurar el sistema cuando se añaden redes
 - Los protocolos se adaptan de forma automática cuando se produce un cambio en los nodos
 - Es flexible ante fallos o caídas en la red
 - Pueden ayudar a controlar la congestión del tráfico
 - Si esta bien diseñado, es menos propenso a errores
 - Escala con mucha más facilidad
 - Inconvenientes: (mensajes sin información de usuario -> información innecesaria)
 - Los nodos necesitan un mayor tiempo de procesamiento por paquete
 - Es necesario intercambiar información sobre el estado de la red entre routers: Mayor carga de tráfico para la red
 - Difícil equilibrio en la velocidad de adaptación a los cambios (cuando se cae una ruta, es complicado avisar que la ruta se ha caído)
 - Clasificación basada en la fuente de información
 - Local: (no son los más óptimos)
 - Los nodos toman las decisiones basándose únicamente en la información que ellos mismos posean
 - Algoritmos de la patata caliente, aprendizaje hacia atrás e inundación
 - Descentralizado:
 - Los nodos utilizan la información recibida de los nodos adyacentes (vecinos) (la información se obtiene de los vecinos)
 - Algoritmos de vector distancia (DS)
 - Global:
 - Los nodos (piden) utilizan la información recibida de todos los nodos
 - Algoritmos de estado del enlace (LS)
- MAYOR CARGA
+ TIEMPO
TARDA EN
AVISAR NODO
CAÍDO

- Algoritmos de encaminamiento

- ~~Busca~~ encontrar la distancia mas corta entre dos puntos
- Los diferentes nodos almacenan información de por donde tienen que enrutar el tráfico
- Las métricas de la distancia pueden ser variables-Retardo, velocidad, distancia...
- Algoritmo de Dijkstra

- Algoritmo de camino más corto



- Algoritmo de la patata caliente → cola menos longitud

- Enviar los datagramas por la cola de menos longitud
 - Equilibra la carga entre las redes
- Combinar la carga de la línea con la dirección preferida de envío
- Es un algoritmo dinámico

- Algoritmo de aprendizaje hacia atrás → cuenta cada salto

- Cada paquete tiene un contador que se incrementa cada vez que da un salto
- Si un nodo recibe un paquete por la línea k de H y tiene un 4 en el contador, sabe que enviando por esa línea H estará como mucho a 4 saltos
- Es un algoritmo dinámico

- Algoritmo de inundación → por todos los sitios menos por el mismo

- Cada nodo envía el paquete por todas las líneas excepto por la que le llegó
- Los paquetes enviados cuentan con un contador que se decremente por cada salto que da
- Se pueden incrementar mejoras para evitar reenviar paquetes repetidos
- El emisor necesita conocer la distancia al receptor, o al menos el tamaño máximo de la red
- Ventajas:
 - Es extremadamente robusto
 - Al menos una copia ha llegado por el camino más corto posible – Puede ser útil para establecer un circuito virtual
 - Se recorren todos los nodos de la red

- Inconvenientes:
 - Se genera una gran cantidad de tráfico

fuentes de información
local
↓
info
entre
mismos
poseen

Dest	Sig salto	Coste
B	B	1
C	C	1
D	B	2

Algoritmo de vector de distancias

- Todos los enrutadores de la red, mantienen una tabla con el resto de nodos de la red, el siguiente nodo de envío y una métrica que indica cuanto tardan en alcanzarlos
- Se pretende encontrar el camino mas corto entre todos los nodos de la red
- Al inicio del algoritmo, los nodos solo conocen la métrica con sus vecinos, mientras que la métrica con el resto se considera infinita
- Los nodos vecinos intercambian información de forma periódica

se adapta,
lento

Red	Sig salto	coste
A	A	1
C	C	1
D	A	1
E	A	2
F	C	3

Algoritmo de estado de enlace

→ fuente información global → de todos los nodos

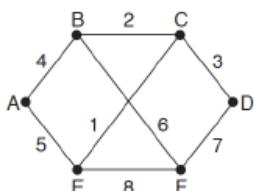
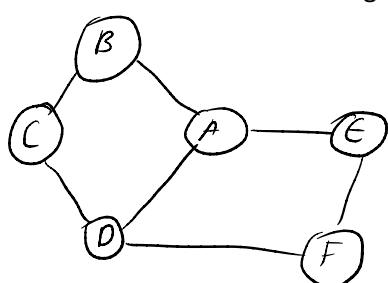
- Es el más utilizado en Internet a días de hoy en sus diferentes variantes
- Sigue cinco pasos:

- Descubrir a los nodos vecinos y conocer su dirección
- Establecer el coste hasta cada uno de ellos
- Crear un paquete para transmitir esa información
- Difundir ese paquete por todas las interfaces
- Calcular la ruta más corta utilizando la información recibida

el que se usa
en internet

- Todos los nodos reciben todos los paquetes
- Es un elemento clave decidir cuándo se reenvía

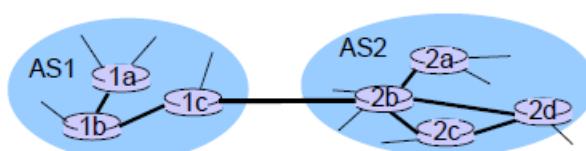
Encaminamiento jerárquico



Enlace		Estado		Paquetes	
A	B	C	D	E	F
Sec.	Sec.	Sec.	Sec.	Sec.	Sec.
Edad	Edad	Edad	Edad	Edad	Edad
B 4	A 4	B 2	C 3	E 5	B 6
E 5	B 5	C 2	D 3	F 7	C 1
		F 6	E 1		F 8

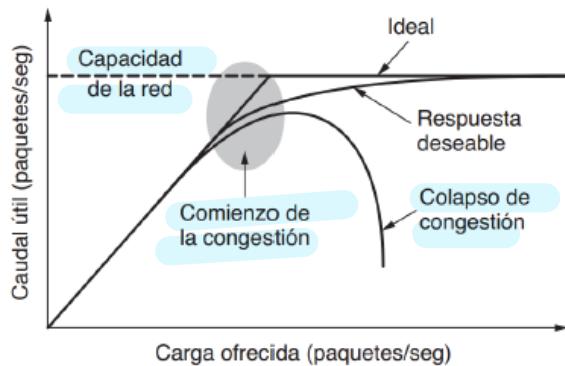
(b)

- Para redes de gran tamaño, no es viable que todos los nodos conozcan a todos
 - Tablas de encaminamiento enormes
 - Sobrecarga de la red por intercambios de vectores
 - Estructuras de red privadas
- Encaminamiento mediante sistemas jerárquicos
- Existen una serie de nodos, que conectan redes entre si
- Puede poseer múltiples niveles y cada uno de ellos utilizar un mecanismo de encaminamiento diferente:
 - Interior Routing Protocol (IGP)
 - Exterior Routing Protocol (EGP)



5. Control de congestión

- **Congestión:** Se produce cuando el tráfico enviado a la red, se aproxima a su capacidad máxima
 - Elevados tiempos de entrega de paquetes
 - Paquetes perdidos o destacados
 - Se produce en un nodo y se propaga hacia atrás



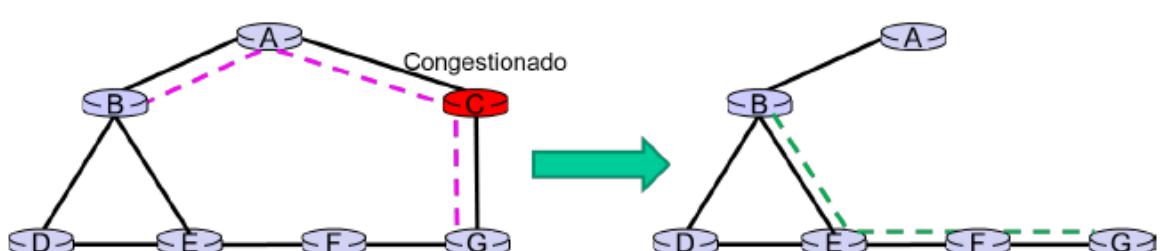
Causas de la congestión

- Los diferentes nodos no tienen capacidad de procesar todo el tráfico
- Las líneas no tienen capacidad para enviar todos los paquetes
- Las colas de los nodos poseen memoria limitada
 - ¿Se solucionaría con colas infinitas?
- Es necesario realizar un control que no sature la red y provoque elevadas pérdidas de rendimiento
- Diferente a control de flujo
 - No afecta solo a los extremos, sino a toda la red
 - Controlar el flujo puede ayudar a controlar la congestión

Métodos de control de congestión

- De ciclo abierto o pasivos
 - Realizar un buen diseño de la red
 - Seleccionar a priori qué tráfico acepta y descartar
 - Regular el tráfico para que sea predecible
 - De ciclo cerrado o activos
 - Las decisiones se toman cuando aparece la congestión
 - Constuye 3 fases:
 - Monitorización
 - Envío de información
 - Ajuste del sistema
 - Activos:
 - Monitorización: Controlar diferentes parámetros de la red
 - Longitud promedio de las colas
 - Nº de paquetes para los que vencen los temporizadores
 - Retardo promedio de los paquetes
 - Porcentaje de paquetes destacados por falta de memoria o capacidad de la red
 - Envío de información: Información a todos los nodos afectados que se produce congestión
- organizarse bien
adaptarse

- Nodo que detecta la congestión envía un paquete especial notificando el programa al origen del tráfico
 - Utilizar un campo (o un bit) del paquete para que los encaminadores avisen de la congestión a sus vecinos
 - Host o encaminadores envían periódicamente paquetes de sondeo preguntando por el estado de la congestión
 - Es muy importante controlar el tiempo de reacción
 - Demasiado pronto: el sistema oscilará y nunca convergerá → no pasó nada
 - Demasiado tarde: el aviso ya no será útil → ya pasó
 - **Ajustes del sistema:** Introducir diferentes cambios en el sistema para reducir la congestión
 - Balancear el tráfico entre rutas
 - Utilizar encaminadores de respaldo, utilizados para la tolerancia a fallos, para encaminar el tráfico
 - Reducir la inyección de paquetes en la red
 - Negación de servicio a usuarios
 - Descartar paquetes
 - Detección temprana aleatoria
 - Random Early Detection (RED)
 - Se aprovecha que para TCM, cuando se pierde un paquete, se reduce el flujo de datos
 - Cuando se reciben señales de congestión en el propio nodo, se empiezan a descartar paquetes de forma aleatoria
 - Al reducirse el tamaño de la ventana de transmisión, se reduce el flujo
 - Suponen una mejora respecto a descartar paquetes cuando se llena el buffer, aunque requieren un mayor ajuste
 - Regulación de tráfico
 - Mantener una tasa de encolamiento baja
 - Es dependiente del tipo de tráfico que se tenga
 - Si se pasa un determinado umbral, se toman medidas
 - Envío de paquetes reguladores, que controlen la cantidad de tráfico que se genera – Puede ser hasta el nodo origen o salto a salto
 - Notificación explícita de congestión (Bit ECN cabecera IP)
 - Control de admisión – Circuitos virtuales
 - No se establecen nuevas rutas hasta que la red pueda trabajar con el tráfico que ya tiene
 - Puede ser complejo estimar la cantidad de tráfico que la red puede manejar, especialmente en el tráfico a ráfagas
 - Se pueden buscar rutas alternativas no congestionadas
- ir viendo como va todo
 alternativas, usar lo que ya tienes



están clasificados, borrar el que convenga

descartar paquetes completos

Desprendimiento de carga

- Es la técnica más agresiva, ya que descarta paquetes completos
- Se aprovecha de la señalización de los paquetes para saber qué tráfico descartar
 - En ciertos casos, es interesante descartar los paquetes más nuevos y en otros, los más viejos
- Los paquetes suelen llevar diferentes categorías de transmisión: Normal, urgente, no descartar...

6. Calidad de servicio (QoS)

- Quality of Service (QoS)

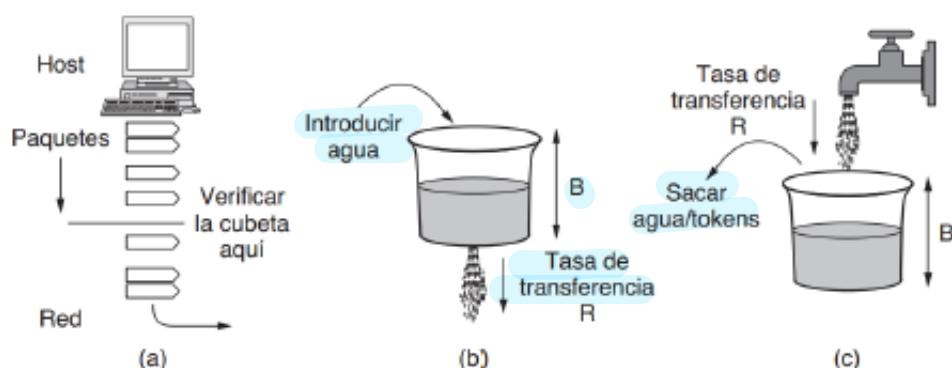
- No todas las aplicaciones pueden utilizar un servicio sin garantía alguna
- La mejor forma de proporcionar una QoS alta es mediante overprovisionamiento – Demasiado caro
- La capa de red puede proporcionar algunas mejoras extra que aumenten la QoS
- Parámetros principales:
 - Ancho de banda
 - Retardo
 - Variación del retardo (jitter)
 - Pérdidas

- Requerimientos de QoS de distintas aplicaciones

Aplicación	Ancho de banda	Retardo	Jitter	Pérdida
Correo Electrónico	Bajo	Bajo	Baja	Media
Compartir archivos	Alto	Bajo	Baja	Media
Acceso Web	Medio	Medio	Baja	Media
Inicio sesión remota	Bajo	Medio	Media	Media
Audio bajo demanda	Bajo	Bajo	Alta	Baja
Vídeo bajo demanda	Alto	Bajo	Alta	Baja
Telefonía	Bajo	Alto	Alta	Baja
Videoconferencia	Alto	Alto	Alta	Baja

- Modelado de tráfico

- Garantizar un tráfico estable pese a las variaciones en la red
- Leaky Bucket y Token Bucket

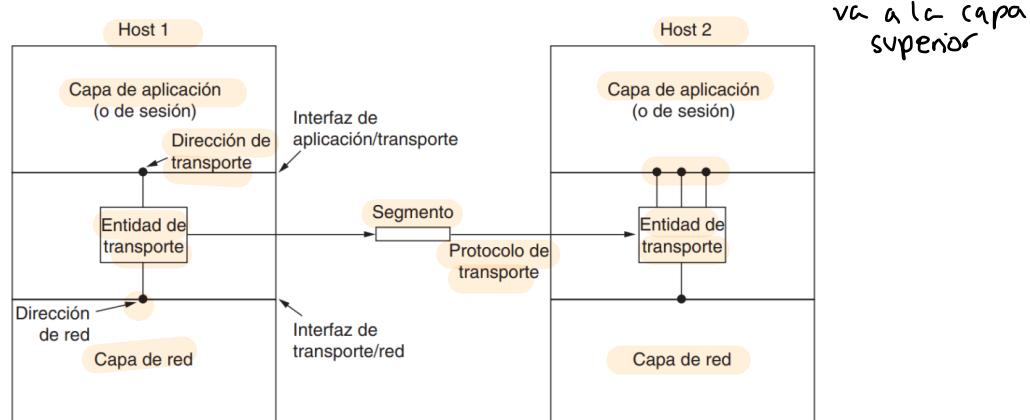


- Gestión de paquetes en cola
 - Métodos FIFO (First Input – First Output)
 - Muy sencillo de implementar
 - Utilizada en el descarte RED
 - No es muy útil para proporcionar una buena QoS
 - Método LIFO (Last Input – First Output)
 - Casi tan simple como FIFO y poco óptimo
 - Permite priorizar el tráfico más reciente – Interesante para aplicaciones de tiempo real
 - Sistemas con prioridad
 - Cada nodo posee varias colas con diferentes prioridades
 - Los paquetes van a cada una de las diferentes colas, en función de la prioridad que tenga
 - Las colas de mayores prioridad se vacían primero
 - Problema: Es posible que las colas con menos prioridad no sean atendidas nunca
 - Encolamiento circular (Round Robin)
 - Todas las tareas van recibiendo el mismo tiempo de procesamiento
 - Una de las implementaciones más comunes
 - Pueden utilizarse variaciones con prioridades, con apropiación, etc.
 - Es el que tiene una implementación más compleja
- Garantía de QoS
 - Es necesario combinar todas las técnicas estudiadas previamente
 - Los algoritmos de encaminamiento basan sus decisiones según los parámetros que posean los diferentes nodos
 - Teoría de colas – Proporciona los retardos promedio en cada nodo en función de la carga
 - Si la red considera que puede gestionar el tráfico y proporcionar la QoS perdida, aceptará la conexión, si no, podrá rechazarla

Tema 5: Nivel de Transporte → segmento (puerto)

1. Introducción

- Proporciona una comunicación lógica entre procesos que se ejecutan en hosts diferentes (comunicación extremo a extremo)
 - Aísla a la capa de aplicación de los detalles de la red o redes intermedias
 - Host origen: divide el mensaje en segmentos y se los pasa al nivel de red → separa y va una capa abajo
 - Host destino: junta los segmentos en mensajes y se los pasa a la capa de aplicación



- Abstracción mediante sockets: Utilización de primitivas para facilitar el diseño y la programación a través de interfaces
 - Se permite el intercambio de datos en ambos sentidos de forma simultánea: full-dúplex
 - Existen dos tipos de protocolos:
 - Orientados a conexión: Segmentos
 - No orientados a conexión: Datagramas
 - Comparación con la capa de red – Host vs Procesos
 - Redundancia de tareas de la capa de enlace:
 - Control de flujo
 - Control de errores
 - Secuenciación
 - Se emplean dos protocolos principalmente:
 - TCP (Transmission Control Protocol)
 - Fiable
 - Entrega de información ordenada
 - Establecimiento de conexión
 - Control de flujo mediante ventana deslizante
 - Control de congestión explícita e implícita
 - UDP (User Datagram Protocol)
 - No fiable
 - Entrega de información no ordenada
- fiável,
 o ordenado,
 ventana
 deslizante,
 congestión
 explícita
 implícita
- no fiable,
 no ordenado

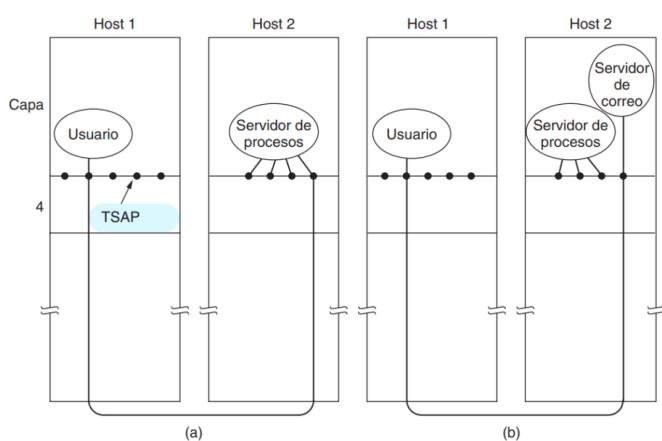
2. Elementos de protocolos de transporte

- Direcciónamiento: conocer el punto de acceso al servicio de transporte (TSAP), que suele ser un número de puerto

↳ n° puerto

Protocolo	Nº de Puerto
20 - 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
443	HTTPS

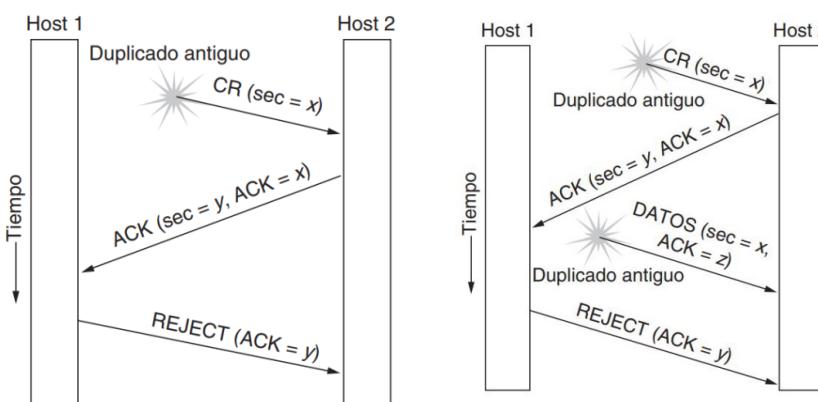
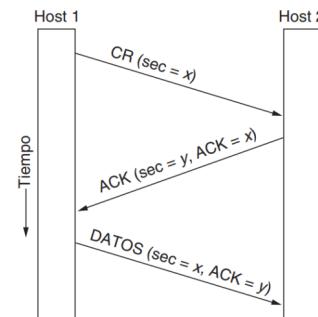
Si el puerto no pertenece a un protocolo conocido, es necesario “negociar” con el host el puerto de acceso: portmapper



- Gestión de la conexión: Problema de los dos ejércitos ¿Podemos asegurar que nuestras comunicaciones llegan?

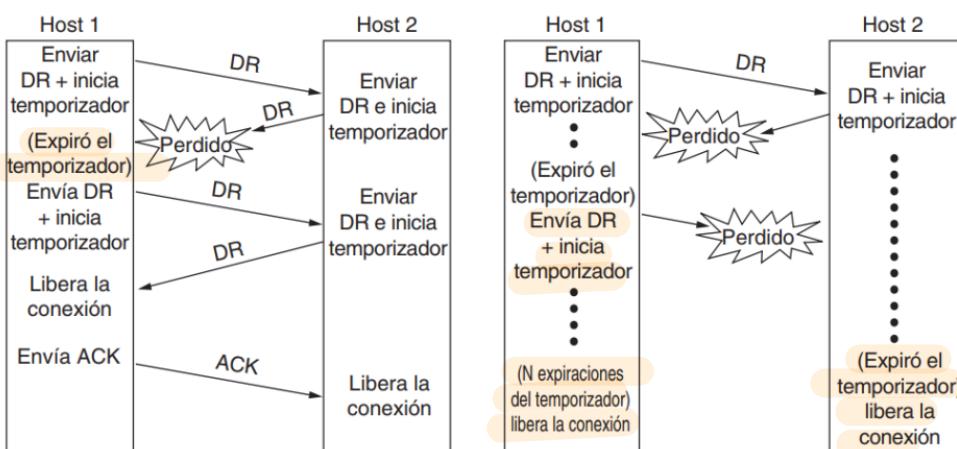
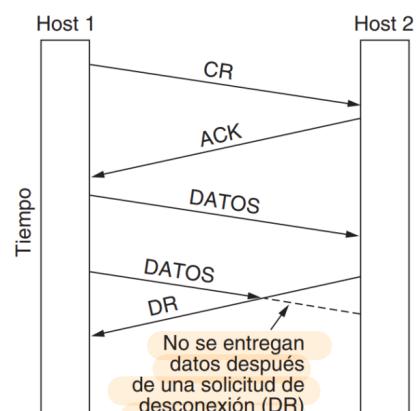
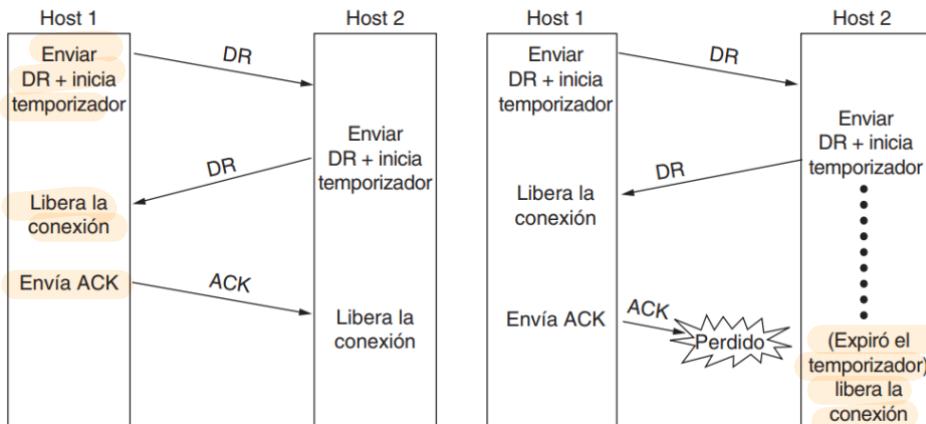
- Establecimiento: Gestión de paquetes perdidos o que llegan con retraso
- Acuerdo de tres vías: Three-way handshake
- Emisor y receptor acuerdan y confirman los número de inicio de secuencia
- Perdida o retraso de los paquetes en el establecimiento

nº inicio
de secuencia



- Liberación de la conexión:

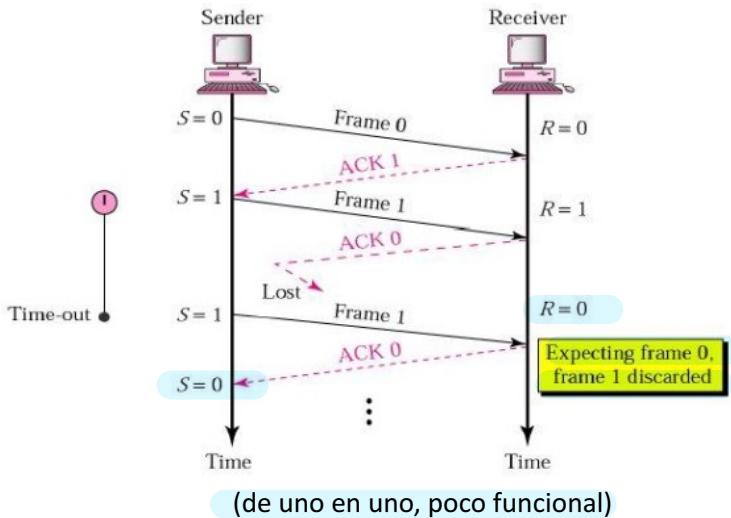
- Asimétrica – Línea telefónica tradicional
- Simétrica – Evitar pérdidas abruptas de datos
- Perdida o retraso de los paquetes en la liberación



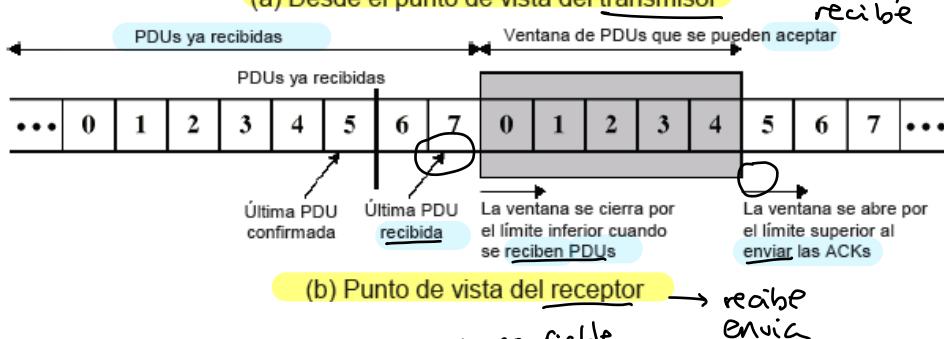
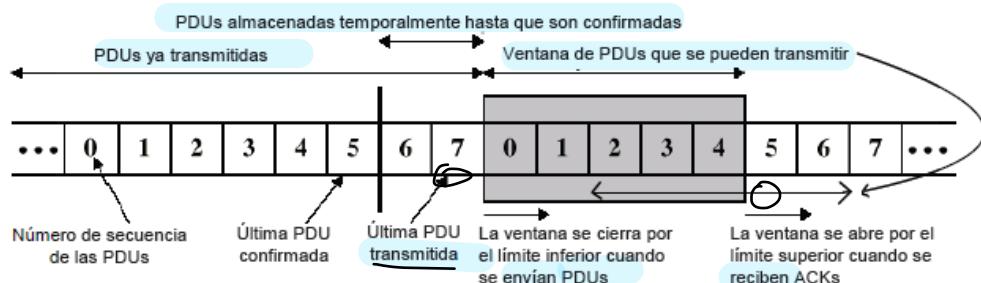
junto con
la capa
anterior
(capa red)

de 1 en 1,
poco
funcional

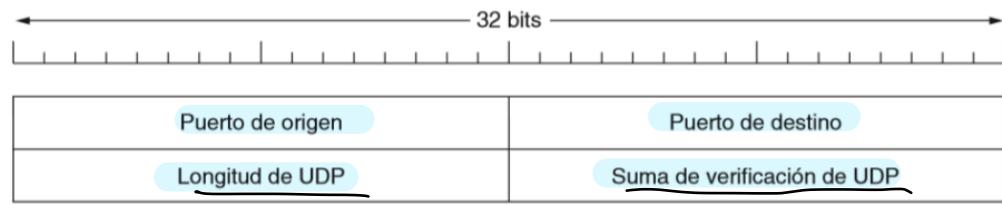
- Control de congestión
 - Evitar la saturación del sistema por enviar una cantidad de paquetes mayor de la que admite
 - Tarea compartida por las capas de red y de transporte
 - Principales causas:
 - Ancho de banda y fiabilidad de la red
 - Capacidad del receptor
- Parada y espera
 - El emisor envía un paquete y espera la confirmación del receptor para enviar el siguiente
 - No son necesarios buffers y únicamente se almacena el último paquete enviado



- Ventana deslizante
 - El emisor mantiene una lista con los W números de secuencia de los paquetes que puede transmitir -> Ventana emisora de tamaño W
 - El receptor mantiene una lista con los W números de secuencia de los paquetes que esta autorizado a recibir -> Ventana receptora de tamaño W
 - Como los paquetes pueden perderse, el emisor guarda una copia de todos los paquetes que están enviados, pero no asentidos por si hay que reenviarlos
 - Asentimientos:
 - Cada asentimiento puede asentir a un grupo de paquetes o hacerlo de forma individual
 - Controlan el flujo y notifican el resultado de las transmisiones de un paquete
 - Indican el número de paquete que se espera en la siguiente transmisión
- resultado,
cuantos
paquetes
esperan



3. El protocolo UDP
- User Datagram Protocol
 - Protocolo no orientado a conexión
 - o Cada segmento se trata de forma independiente de los demás
 - Es un protocolo no fiable -> ofrece un servicio "best effort"
 - o Sus mensajes pueden llegar fuera de secuencia o perderse
 - No se envían asentimientos: se reduce el tráfico de la red
 - No controla la congestión
 - Reduce la información suplementaria a enviar
 - (TCP->HTTP; TCP-(ahora se usa)->UDP -> HTTP)
 - Proporciona interfaz intermedia entre la capa de aplicación y la de red
 - o Gestión del uso de los puertos (MACs, IPs)
 - o Pueden proporcionar control de errores (Enlace y transporte -> menos probable errores)
 - Adecuado para situaciones con requisitos de conexión bajos
 - o Servicio DNS
 - o Video bajo demanda
 - o Radio en Internet
 - o Telefonía en Internet
 - o Algunos modelos cliente-servidor
 - Cabecera UDP (8 bytes)

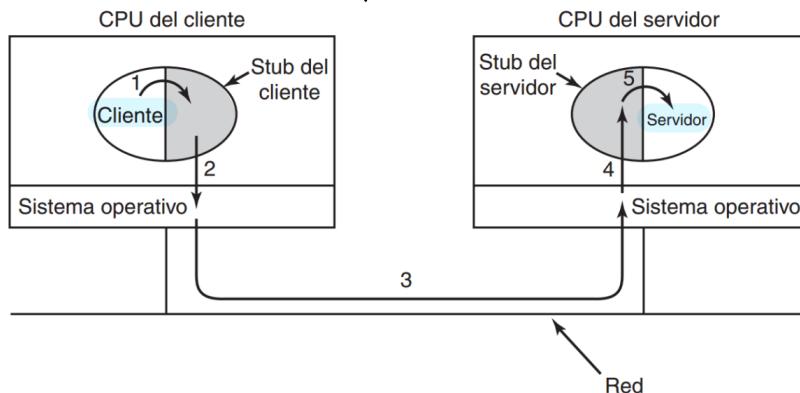


- longitud
- suma verif.

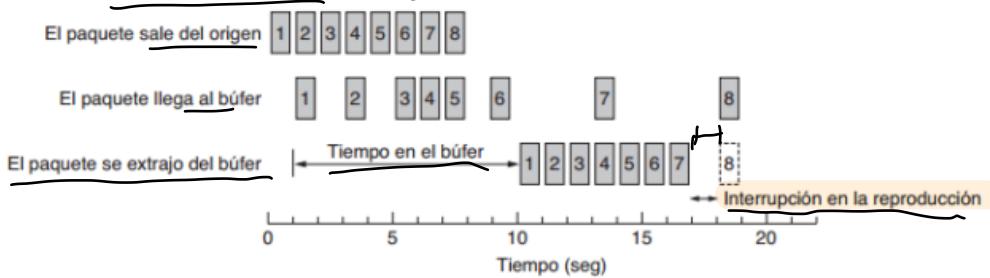
- Puerto de origen: contiene el numero de puerto por si es necesario responder al origen
- Puerto de destino: contiene el numero de puerto del destino
- Longitud: longitud de los datos del datagrama IP
- Suma de comprobación: asegura la integridad del datagrama. Se calcula utilizando la cabecera UDP y el campo de datos

UDP + Datos → comprobación

- Remote Procedure Call (RPC)
 - Hacer que una llamada a un procedimiento remoto sea parecida a un procedimiento local *parece local pero es remoto*



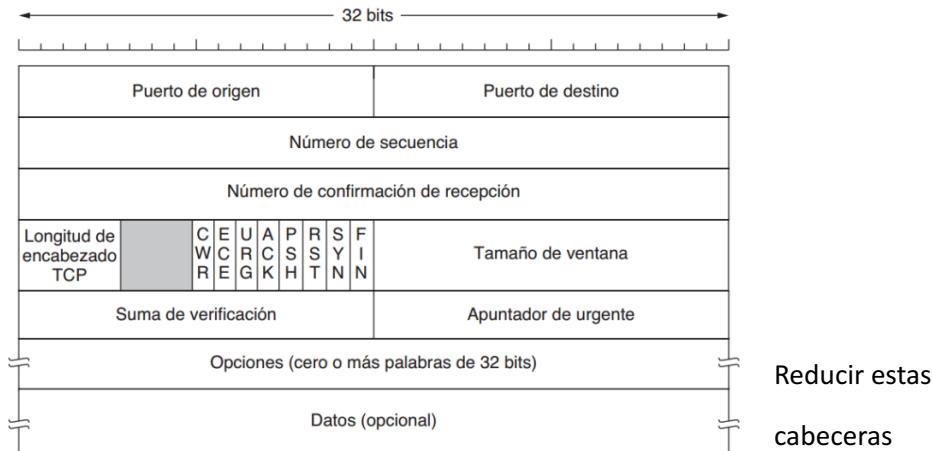
- Real-time Transport Protocol (RTP)
 - Está ubicado justo por encima de UDP en la capa de transporte
 - Se suele utilizar en la transmisión de paquetes de audio y video en tiempo real
 - Puede ser unidifusión o multidifusión
 - Los número de paquetes son incrementales y consecutivos
 - Puede transmitir información relacionada a través de varios flujos
 - Utiliza las estampas de tiempo (timestamping) (en qué orden y en qué tiempo) para sincronizar los diferentes flujos y reducir la variación de retardo o jitter
 - Empleo de buffers para el control del tráfico



4. El protocolo TCP (orientado a conexión, fiable)

- Transmission Control Protocol
- Protocolo orientado a conexión:
 - 3 fases: establecimiento de conexión, transferencia, cierre de conexión
- Proporciona una capa fiable por encima del protocolo IP:
 - Se utilizan asentimientos (ACK)
 - Sigue reenvíos
- Se encarga de fragmentar la información que recibe del nivel superior (TCP pega los mensajes, IP no tiene que realizarlo)
 - Tamaños máximos de 64 KB
 - Habitualmente 1460 bytes
- Emplea puertos que son llamados a través de sockets
- Utiliza un sistema de ventana deslizante para el control de flujo a este nivel
- Utiliza buffers para transferencia haciéndola más eficiente
 - Acumula datos hasta que tiene suficientes para llenar un datagrama
 - También se puede forzar el envío

- Se intercambian flujos de bytes, divididos en segmentos
- Realiza control de la congestión a nivel de transporte. Se necesitan algoritmos diferentes a los utilizados en niveles más bajos
- Switches, routers, hubs, no hay transporte de información
- Cabecera TCP

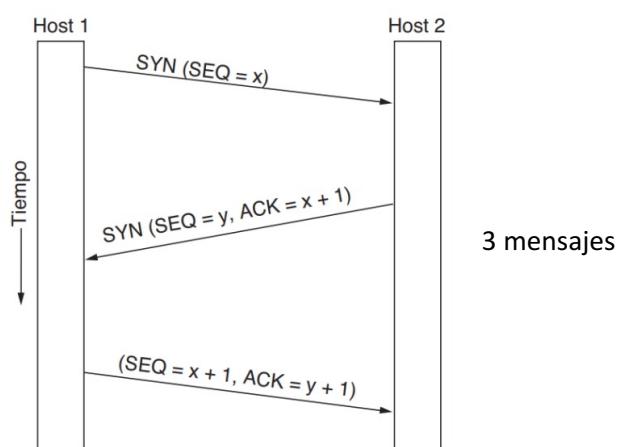


- Puerto de origen y destino: contiene los números de los puertos de envío y recepción
- Número de secuencia: identifica el número de secuencia del primer byte de datos del segmento. Si es un segmento SYN, es el número de secuencia inicial
- Número de confirmación de recepción: indica el número del siguiente byte que se desea recibir, no el último byte recibido
- Longitud encabezado: cantidad de palabras de 32 bits incluidas en el encabezado
- Campo reservado para posibles usos
- CWR (Congestión Window Reduced): bit para indicar reducción del tamaño de la ventana (por culpa de la congestión, envía un mensaje para que no hagas la ventana más grande)
- ECN (Explicit Congestion Notification): identificador que se utiliza para indicar que se está congestionando la red
- URG(Urgent): utilizado para indicar que el valor del campo "apuntador de urgente" es válido
- ACK (Acknowledgment): se utiliza para indicar que la respuesta también confirma datos recibidos
- PSH(Pushed Data): indica la entrega inmediata de los datos al nivel superior. No se espera a que se llene el buffer (forzar a que se pase al nivel superior el mensaje junto con el buffer)
- RST (Reset): empleado para reiniciar la conexión (tamaño ventana (según el control de flujo) ≠ nº de la secuencia)
- SYN (Synchronize): se utiliza para establecer la conexión. Únicamente los primeros mensajes tendrían este bit a 1 (se está estableciendo la conexión)
- FIN: corta la conexión y es el último mensaje enviado por cada transmisor
- Tamaño de ventana: indica el tamaño de la ventana. Puede ser igual a 0 (según las situaciones, asentir un mensaje, pero no se quiera enviar más)

- Suma de verificación: sirve para comprobar que el mensaje se ha transmitido sin errores
- Apuntador de urgente: es un offset que permite conocer el ultimo valor de byte de los datos urgentes (trozo urgentes y se enumeren los trozos)
- Options: permite definir nuevas opciones que no estén entre las incluidas por defecto en la cabecera
 - Tamaño máximo del segmento
 - Escala de ventana (multiplica el tamaño de la ventana)
 - Estampa de tiempo
 - Selective ACK

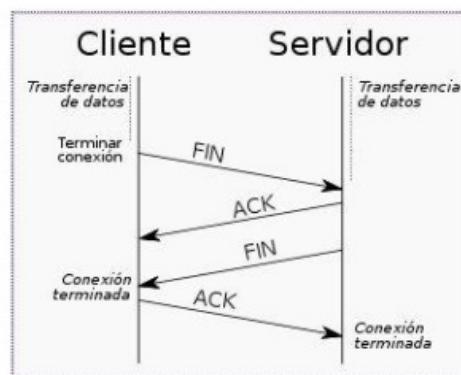
- **Establecimiento de conexión**

- Handshake de triple vía
apertura de la conexión



- **Cierre de conexión**

- Handshake de cuatro vías

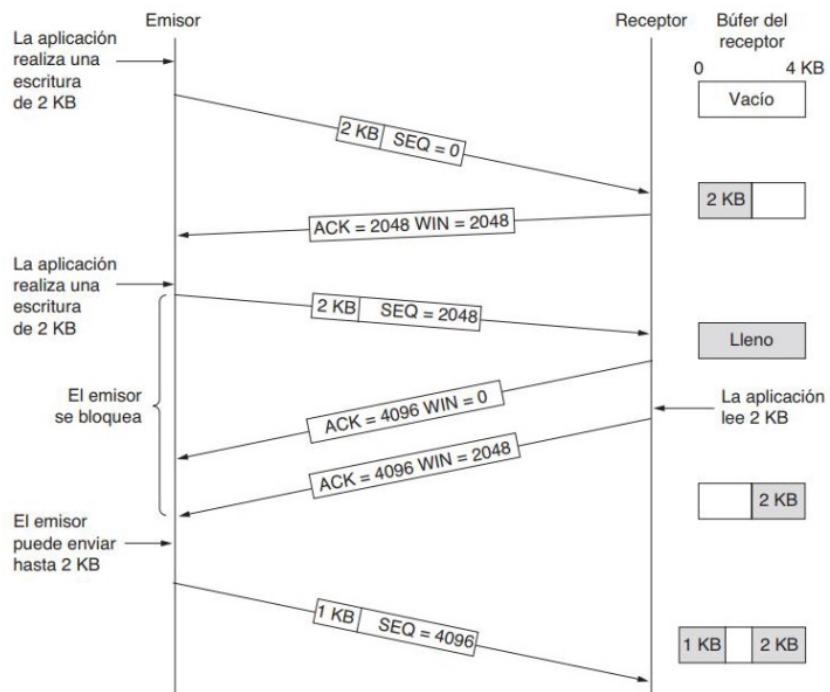


Si no recibe, después de un tiempo, la conexión se cortará, aquí espera para rechazar el ping

- **Fiabilidad en el protocolo TCP**

- Perdida de segmentos:
 - Los segmentos tienen número de secuencia
 - Se responderá a la llegada de segmentos correctos mediante asentimientos (ACK)
 - Los asentimientos hacen referencia al flujo de bytes recibidos, no a segmentos individuales

- Se utilizarán temporizadores para controlar la perdida de tramas: retransmisión
- Duplicados:
 - Cuando TCP considera que se ha perdido un segmento enviará un duplicado
 - El receptor detectará el doble envío gracias al número de secuencia y descartará la trama
- Eficiencia y control de flujo:
 - Se utiliza un sistema de ventana deslizante para gestionar el flujo
 - Se utiliza un tamaño de ventana variable controlado por el receptor
 - Se utiliza el sistema de superposición para el ahorro de ancho de banda consumido por los ACKs
- Control de errores:
 - Entrega los datos sin errores
 - Suma de comprobación
- Control de flujo mediante ventana deslizante
 - La ventana es de tamaño variable y está controlada por el receptor
 - No controla el número de segmentos recibidos, si no el número de bytes
 - Ventana del emisor: número de bytes que puede enviar sin recibir asentimiento
 - Ventana del receptor: número de bytes que puede aceptar
 - Las respuestas transportan el número de bytes recibidos correctamente y el tamaño de la ventana receptora, que puede aumentar o disminuir
 - Se pueden realizar asentimientos acumulativos con el objetivo de reducir el ancho de banda utilizado



- Los datos con el flag URG siempre pueden enviarse
- Si la ventana está llena, puede enviarse un segmento de tamaño 1 byte

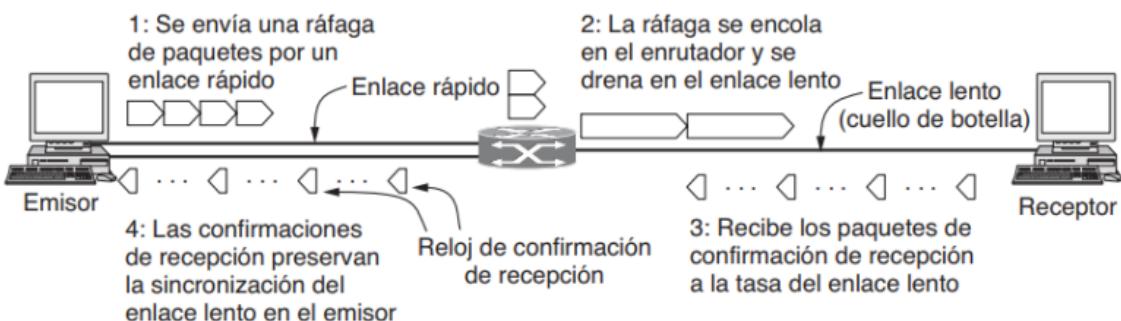
- Algoritmo de Nagle: Adecuado para situaciones de envío con paquetes pequeños
 - Se envía el primer segmento de información que llegue
 - La nueva información se almacena en un buffer hasta que llegue la confirmación del anterior segmento
 - Reducir el gasto de ancho de banda por culpa de las cabeceras

- Control de la gestión

- El reloj de confirmación de recepción (ack clock)
- Utilización de temporizadores para evitar sobrecargar la red
- Ventana de congestión
- Algoritmo de control:
 - Inicio lento
 - Retransmisión rápida
 - Recuperación rápida
 - Asentamientos selectivos

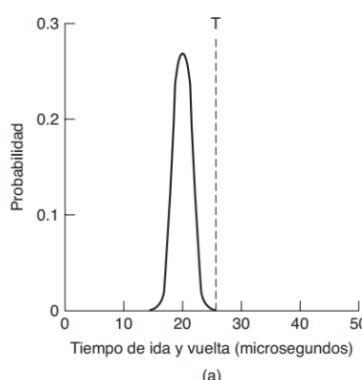
- Control de la congestión – Ack clock

- La velocidad de la red por la que se emite, está limitada por su enlace más lento
- El emisor necesita adaptar su velocidad a la máxima permitida por dicho enlace
- Se utiliza el llamado reloj de confirmación de recepción o ack clock

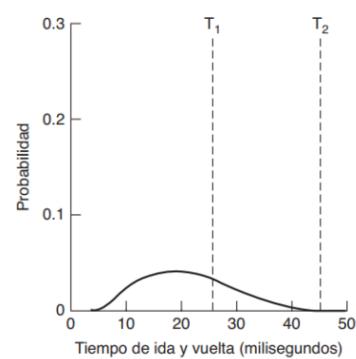


- Control de congestión – Temporizadores

- Retransmission TimeOut (RTO)
 - Tiempo que se espera antes de reenviar un segmento
- $RTO = \text{Tiempo medio de ida y vuelta} + 4 \cdot \text{desviación media}$



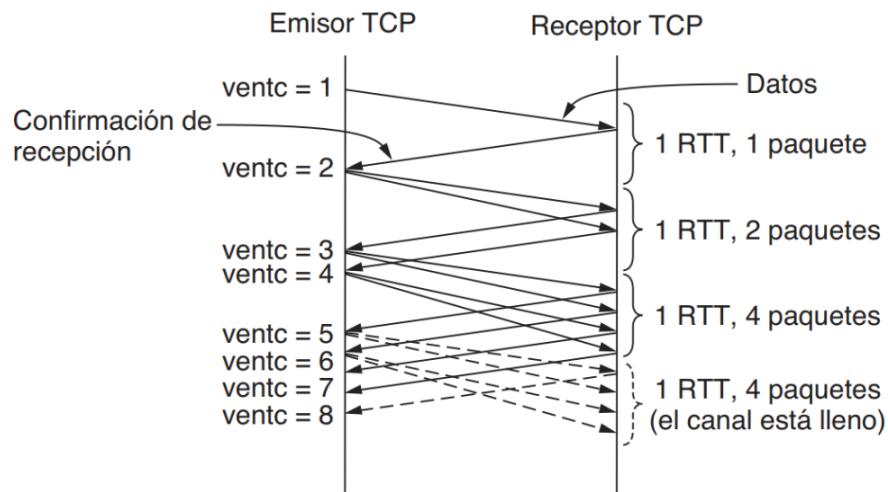
(a)



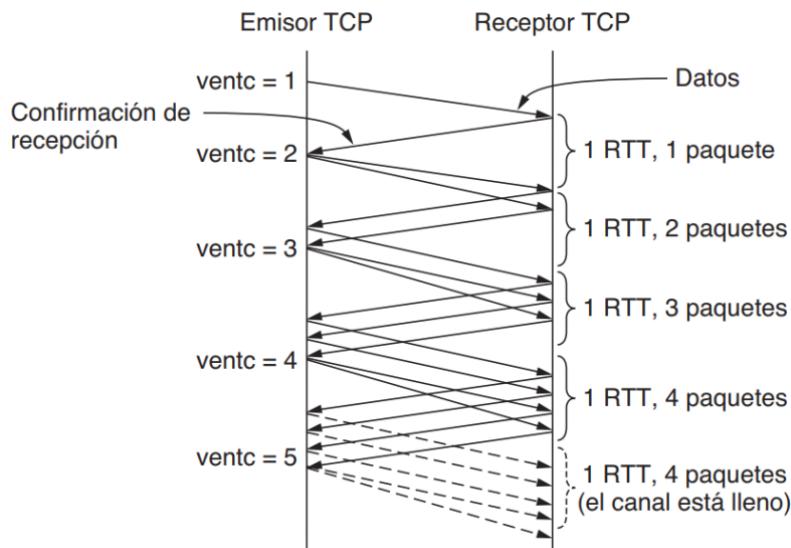
(b)

- Temporizador de Persistencia
 - El receptor envía un ACK con tamaño de ventana 0
 - Cuando actualiza el tamaño de ventana, el paquete se pierde

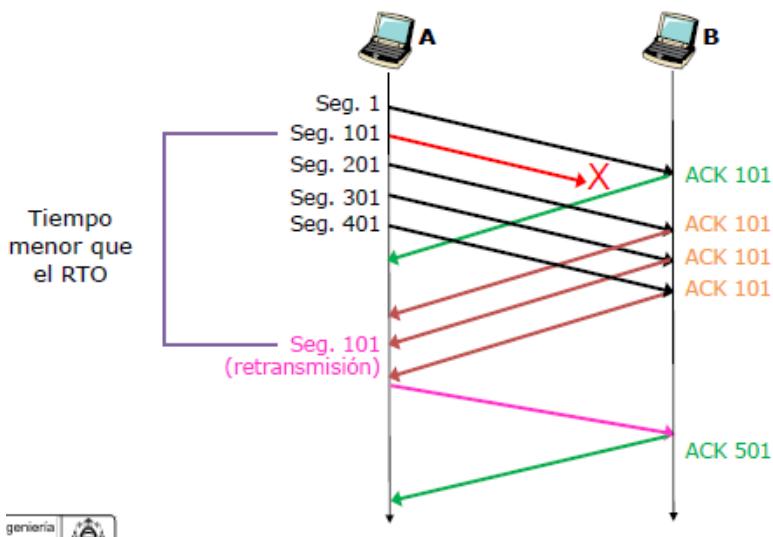
- El emisor envia un mensaje de sondeo para forzar que el receptor le confirme el tamaño de la ventana
- Temporizador Keep Alive
 - Despues de tiempo sin mensajes, una de las partes envia un mensaje vacío para confirmar que el otro extremo sigue activo
- Control de congestión- Ventana congestión
 - Es el máximo numero de bytes que el emisor puede poner en la red
 - Funciona en paralelo con la ventana deslizante del control de flujo – El valor mas pequeño de ambas se corresponde con el valor de la ventana que se vaya a utilizar
 - Hay que obtener su valor optimo para evitar saturar la red
 - El valor ideal puede variar y es necesario que la ventana se adapte a dicho tamaño
 - Se intentan utilizar reglas AIMD (Additive Increase Multiplicative Decrease)
- Control de congestión – Inicio lento
 - Al inicio de la transmisión, se envía un único segmento
 - Una vez que llega correctamente la confirmación, se envían dos segmentos
 - Cuando llegan nuevamente las confirmaciones, se duplica de nuevo el tamaño de la ventana – cuatro segmentos
 - La operación se repite hasta que ocurra algún evento que indique que hay congestión en la red
 - Incremento exponencial – La ventana de congestión puede crecer muy rápido



- Un crecimiento excesivamente rápido, hace que sea muy difícil encontrar el tamaño de ventana ideal
- Se puede establecer un umbral de inicio lento, a partir del cual el incremento pasa a ser lineal y no exponencial
- Cada vez que llegan todas las confirmaciones, el tamaño de la ventana se incrementa en un solo segmento en lugar de duplicarse
- Este umbral va aumentando cada vez que aumenta el tamaño de la ventana
- Esto permite encontrar de una forma mas precisa el tamaño ideal de la ventana

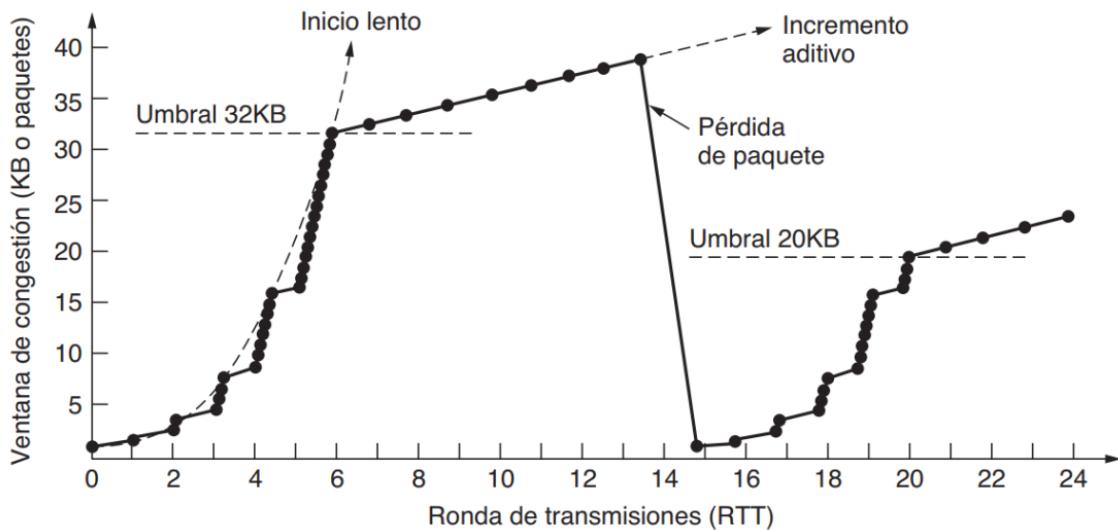


- Control de congestión – Perdida de paquetes
 - ¿Cómo detectar que se pierde un paquete?
 - Salta uno de los temporizadores RTO – Se considera que el paquete se ha perdido o que llegara demasiado tarde
 - Se reciben tres asentimientos repetidos
 - Están llegando segmentos nuevos al receptor, pero falta uno de los anteriores
 - El emisor no espera a que salte el RTO para enviar de nuevo el paquete, lo reenvía al recibir el tercero ACK repetido
 - Retransmisión rápida



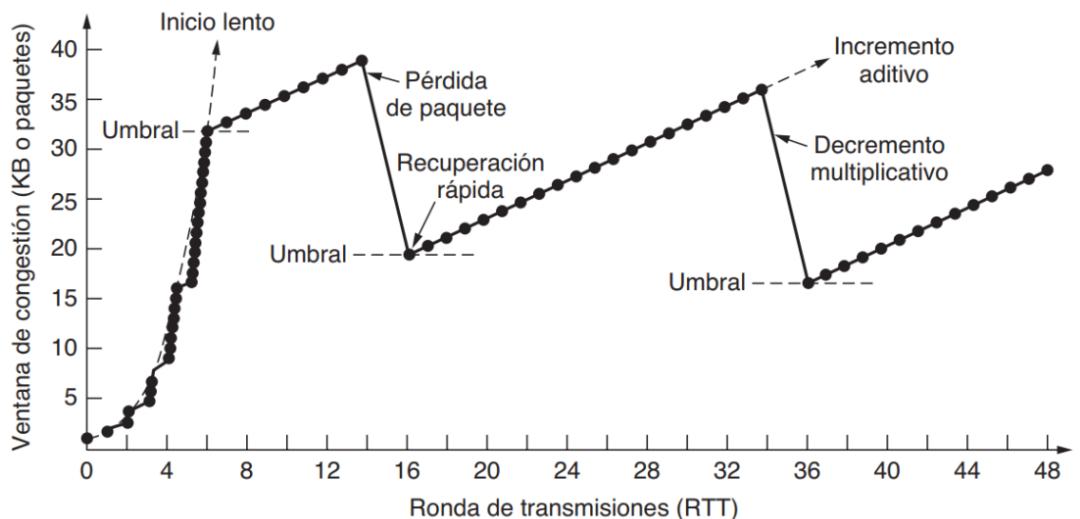
- ¿Cómo actuar cuando se pierde un paquete?
 - Reiniciar el valor de la ventana de congestión
 - Dividir entre dos el valor del umbral de inicio lento
 - Repetir el proceso para ir aumentando el valor de la ventana hasta que puede volver a parecer congestión
- Control de congestión – TCP Tahoe
 - Implementar inicio lento

- Utilizar umbral de inicio lento
- Detectar perdida de paquetes mediante RTO y ACKs repetidos
- Cuando se pierde un paquete, reiniciar el valor de la ventana de congestión a un segmento y el umbral de inicio lento a la mitad del valor actual



- Control de congestión – Recuperación rápida

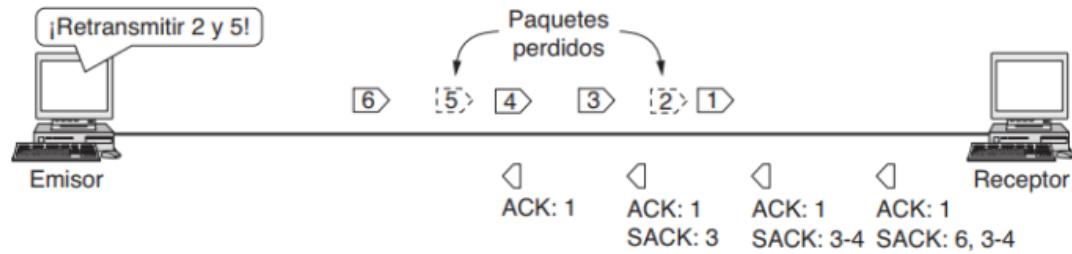
- Se detecta que hay congestión en la red
- El valor de la ventana de congestión se reinicia
- No se utiliza una ventana de tamaño uno, sino una nueva ventana con la mitad del tamaño que la actual
- Como el umbral de inicio lento tiene ese valor, los nuevos incrementos son lineales, no exponenciales
- Algoritmo TCP Reno



- Control de congestión – Asentimiento selectivo

- El campo ACK de la cabecera, indica el último paquete que se ha recibido en orden y correctamente
- Mediante el campo "options" se pueden hacer asentimientos selectivos de tramas que llegan fuera de orden

- Se pueden agrupar paquetes consecutivos que puedan haber llegado fuera de orden
- Ayuda en la velocidad de recuperación ante perdidas, pero es un complemento a las técnicas anteriores



- **Problemas y futuro**

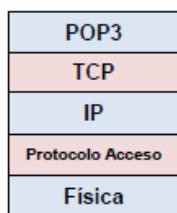
- Desarrollado en los 80, apenas ha sufrido cambios significativos
- El aumento de las velocidades de las redes ha supuesto un problema importante
- Debido a su amplia implementación, es muy complicado cambiar por nuevos protocolos
- El control de la congestión aún debe ser mejorado

Tema 6: Nivel de aplicación

1. Introducción

- Esta formado por un conjunto de protocolos:
 - Cada uno de ellos se utiliza para un propósito específico
 - Cada uno de los protocolos es independiente
 - Puede convivir varios dentro de una red y dispositivos
 - Son utilizados para aplicaciones a las que se denomina servicios
 - Utilizan servicios extremo a extremo del nivel de transporte

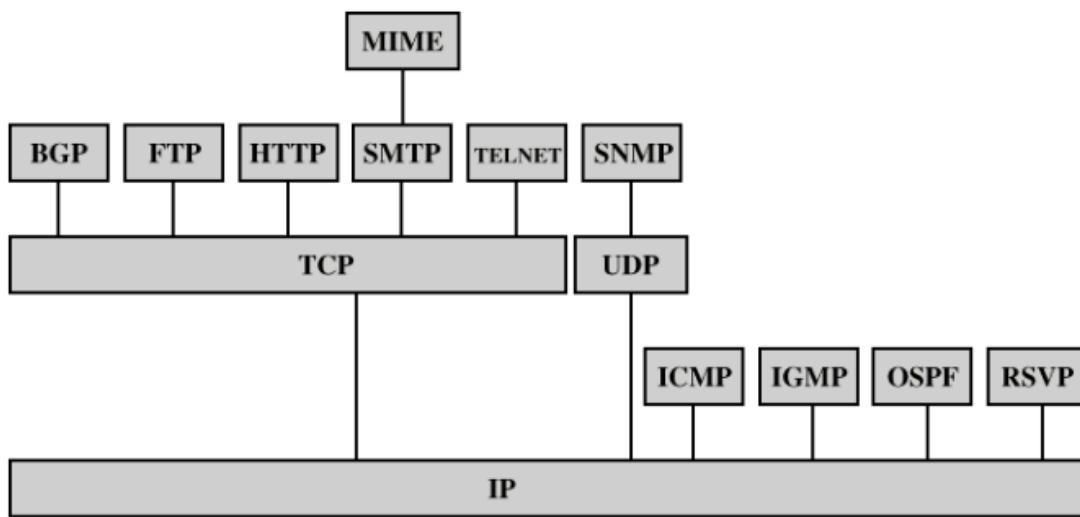
- **Ejemplo de protocolo de nivel de aplicación**



```

Servidor: +OK Hello there.
Cliente: USER alumno
Servidor: +OK Password required.
Cliente: PASS Pass_Alumno
Servidor: +OK logged in.
Cliente: STAT
Servidor: +OK 1 15216
Cliente: LIST
Servidor: +OK POP3 clients that break here, they violate STD53.
1 15216
.
.
.
Cliente: RETR 1
Servidor: +OK 15216 octets follow.
Date: Mon, 04 Dec 2006 20:00:57 +0100
From: Profesor <profesor@uniovi.es>
Subject: Prueba e-mail
To: alumno@uniovi.es
...
.
.
.
Cliente: DELE 1
Servidor: +OK Deleted.
Cliente: QUIT
Servidor: +OK Bye-bye.

```



BGP = Border Gateway Protocol

FTP = File Transfer Protocol

HTTP = Hypertext Transfer Protocol

ICMP = Internet Control Message Protocol

IGMP = Internet Group Management Protocol

IP = Internet Protocol

MIME = Multi-Purpose Internet Mail Extension

OSPF = Open Shortest Path First

RSVP = Resource ReSerVation Protocol

SMTP = Simple Mail Transfer Protocol

SNMP = Simple Network Management Protocol

TCP = Transmission Control Protocol

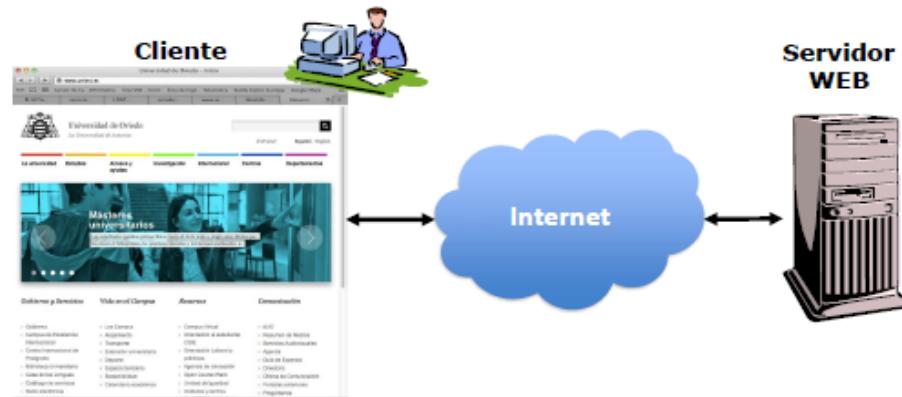
UDP = User Datagram Protocol

2. Ejemplos de protocolos de nivel de aplicación

- Protocolos de servicios orientados al usuario

 - o HTTP

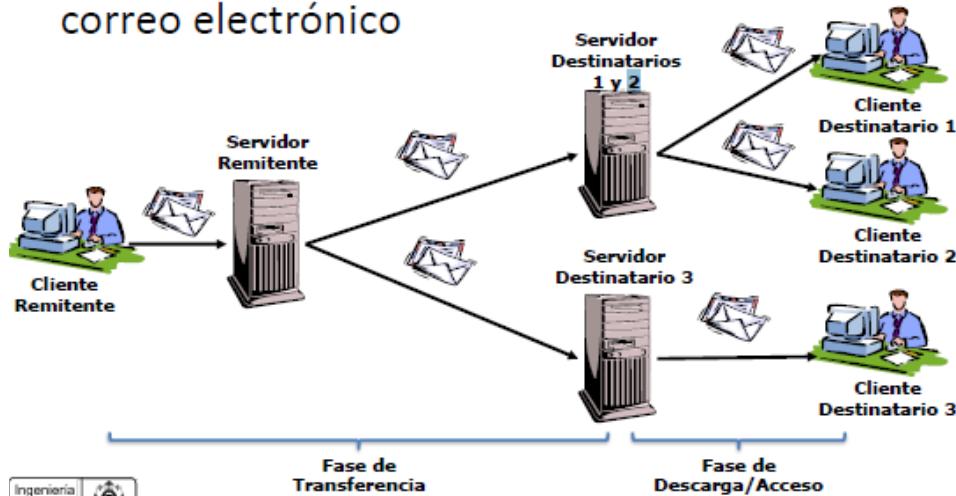
 - Protocolo para transferencia de ficheros de hipertexto
 - Base para los servicios Web
 - Sobre una capa de cifrado se le conoce sobre HTTPS



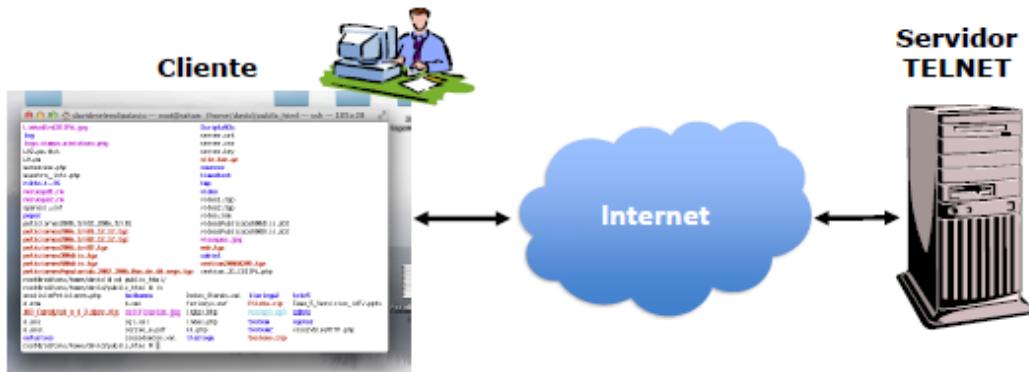
 - o SMTP, POP3, IMAP

 - Protocolos para el envío de mensajes de correo electrónico

correo electrónico



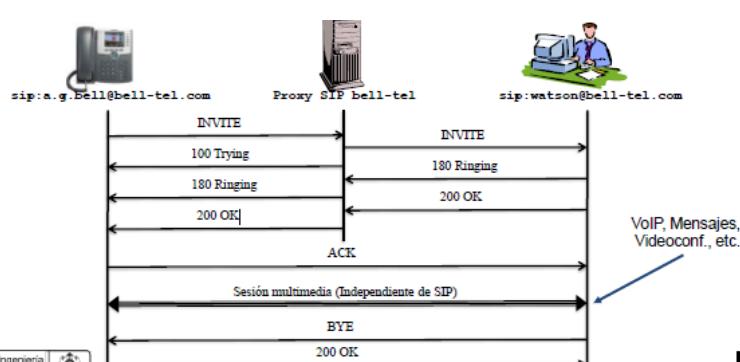
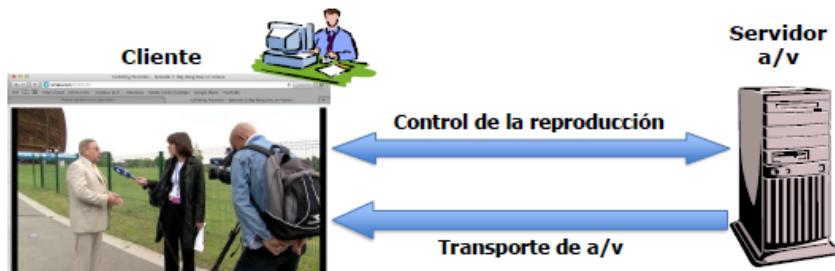
- TELNET, SSH
 - Protocolos para el trabajo mediante terminal remota
 - Permite trabajar desde una localización remota con la consola de un computador



- RFB, ICA, RDP
- FTP
 - Protocolo utilizado para transferencia de archivos entre maquinas remotas

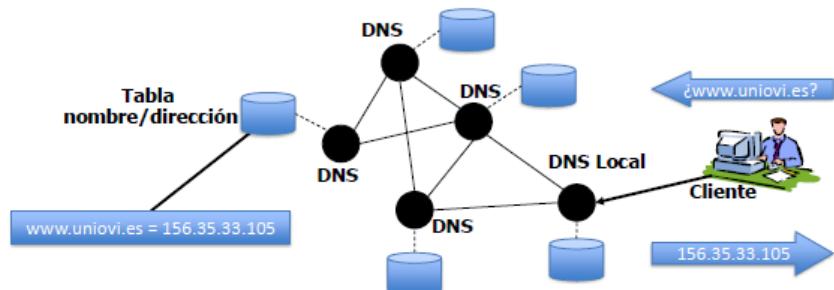


- RTSP
 - Protocolo para el control de servicio multimedia basados en tecnología de streaming
 - Únicamente realiza el control del sistema
 - Utiliza otros protocolos para el transporte de la información

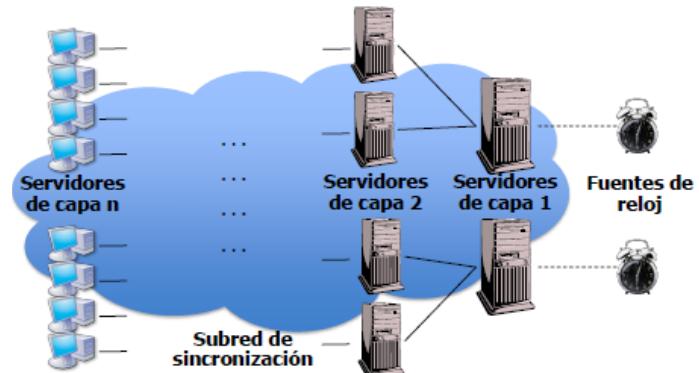


- SIP
 - Protocolo de control y señalización para la creación, modificación y finalización de sesiones de uno o más participantes
 - Sesión: llamada de VoIP, mensajería, videoconferencia, ...

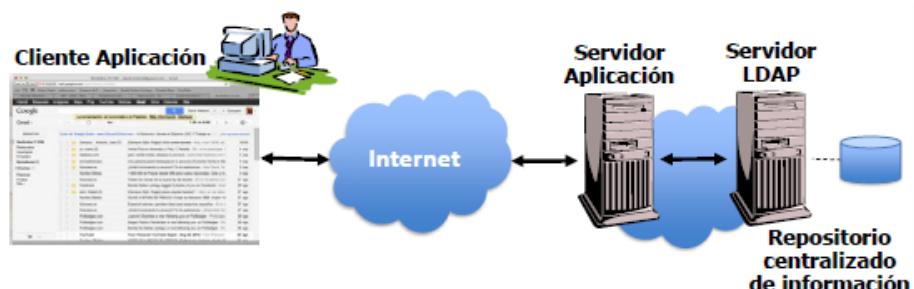
- ...
 - (Utilizados por servicios a los que el usuario accede directamente)
- Protocolos de servicios básicos
 - DNS
 - Protocolo para la resolución de nombres
 - A partir del nombre lógico de una máquina resuelve su dirección IP



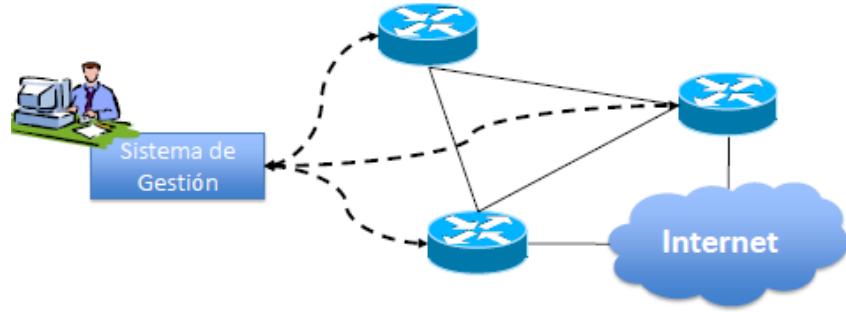
- DHCP
 - Protocolo para el reparto de direcciones IP de forma dinámica
- NTP
 - Permite el acceso y la distribución de señales de reloj precisas



- LDAP
 - Implementa un servicio de directorio
 - Altamente optimizado para lectura de datos

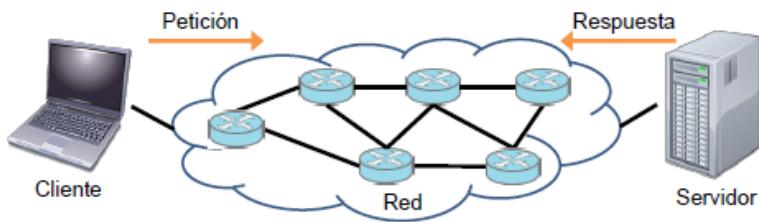


- SNMP
 - Protocolo para la gestión de red
 - Monitorización y control



- ...
 - (Utilizados por servicios base para el funcionamiento de la red o de otros servicios)

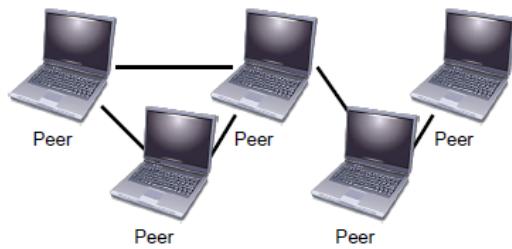
3. El modelo cliente/servidor



- Programa Servidor: ofrece un servicio y acepta peticiones de clientes
- Programa Cliente: se comunica con el servidor para solicitar un servicio
- Ejemplo simple
 - Consideraremos un servidor de eco basado en UDP
 - El servidor seguirá el siguiente proceso:
 - Negociará con el Sistema Operativo un puerto UDP
 - Entrará en un ciclo sin fin con las siguientes tareas:
 - Espera a que un datagrama llegue al puerto de eco
 - Invierte las direcciones de origen y destino
 - Devuelve el datagrama al emisor original
 - El cliente seguirá el siguiente proceso:
 - Envía un mensaje al programa servidor de eco
 - Espera la respuesta
 - Características del servidor
 - Host siempre disponible
 - Dirección IP y puerto bien conocido
 - Su ejecución debe comenzar antes que la ejecución de los clientes
 - Puede atender a varios clientes
 - Características de cliente
 - Es el que inicia la comunicación con el servidor
 - Puede tener dirección IP dinámica y puerto aleatorio
 - No se comunica directamente con otro cliente

- Complejidad en los servidores
 - o Habitualmente los servidores no son tan sencillos como el del ejemplo:
 - Procesamiento de peticiones de forma concurrente
 - Aspectos relacionados con la seguridad
 - o En cuanto a la concurrencia, los servidores suelen tener dos partes:
 - Un proceso maestro sencillo, responsable de aceptar las nuevas peticiones
 - Varios esclavos, responsables de manejar cada una de las peticiones
 - o Técnicas de gestión de esclavos:
 - Esclavos por petición: cada vez llega una petición se crea un esclavo para procesarla
 - Esclavos por sesión: cada vez que se inicia una sesión se crea un esclavo para gestionarla (una sesión contiene una o varias peticiones)
 - Conjunto de esclavos: el servidor tiene inicialmente un conjunto de esclavos activos inicialmente que va repartiendo según llegan las peticiones. Cuando estas terminan los esclavos se liberan (pero no se destruyen).
 - Conjunto de esclavos con asignación por petición
 - Conjunto de esclavos con asignación por sesión
 - o Problemas de seguridad
 - Protección del sistema y de los recursos
 - Deben mantener reglas de autorización y protección
 - Restringir el acceso a ciertas zonas
 - Integridad
 - Deben protegerse contra peticiones formadas equivocadamente y contra peticiones que causen la interrupción del programa
 - o Las arquitecturas de los servidores pueden ser más complejas
 - Reducir el consumo de recursos
 - Garantiza la disponibilidad del servicio
 - Garantiza la escalabilidad del servicio
 - Incrementar la seguridad del servicio
 - o Otros elementos:
 - Caches
 - Proxies
 - Repartidor de carga
 - Firewalls, IDS e IPs
- 4. Arquitectura centralizada – Servidores y nube
 - El cliente puede delegar parte de sus funciones en el servidor
 - o Videojuegos en streaming
 - o Comandos de voz telefonía móvil
 - La mayoría de servicios se trasladan al servidor
 - Mayor necesidad de recursos y estabilidad – Computación en la nube
 - Servicios en la nube
 - o Ventajas
 - Facilidad de escalado

- Posible ahorro económico
 - Delegación de problemas técnicos: PaaS (Platform as a Service)
 - Inconvenientes
 - No se tiene acceso físico a los servidores
 - Cesión la información del servidor a terceras empresas
5. Arquitectura distribuida – El modelo P2P
- Distribuye la información en vez de concentrarla en un servidor
 - Se consideran todos los nodos iguales a la hora de compartir la información
 - Todos los nodos pueden dar y recibir
 - No existe un proveedor centralizado
 - Las comunicaciones son simétricas



- Ventajas
 - Escalabilidad: Es muy fácil unir nuevos nodos
 - Descentralización: La información no se almacena únicamente en un servidor
 - Coste: El gasto se reparte entre los diferentes nodos
 - Robustez: No hay un único punto de fallo
- Inconvenientes
 - La información está distribuida entre múltiples nodos que a priori desconocemos
 - Un nodo malicioso puede causar grandes problemas a toda la red
- P2P: Funcionamiento básico
 - Se localizan otros pares que tengan la información deseada → proveedores
 - Herramientas de búsqueda, información en la web, servidores centralizados, superpares, ...
 - Se descarga la información
 - Si hay más de un proveedor la información se divide en porciones y se descarga cada porción de un par
 - Se cede la información tan pronto como se tenga