Administración avanzada de redes y servidores

Dispositivos hardware de la capa de enlace de datos. Switches.

Área de Ingeniería de Sistemas

Profesor:

Carlos Elvira Izurrategui

Capa de enlace de datos.

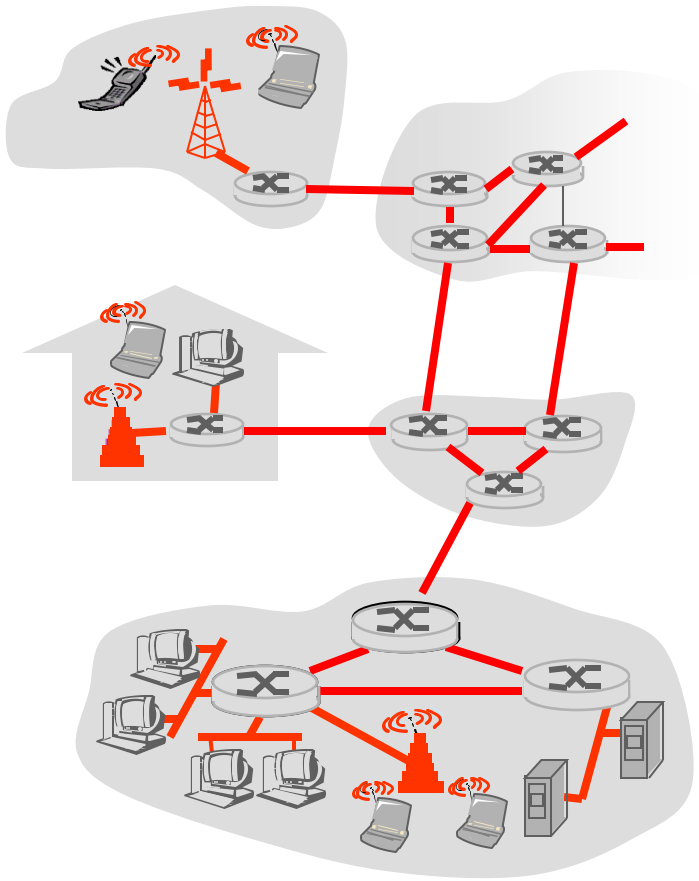
- Objetivos:
  - Conocer los principios básicos que subyacen en los servicios disponibles en la capa de enlace de datos.
    - Detección de errores.
    - Corrección de errores.
    - Acceso múltiples a un canal de difusión compartido.
    - Direccionamiento en la capa de enlace.
    - Transferencia de datos fiable.
    - Control del flujo
  - Instalación e implementación de tecnologías utilizadas en la capa de enlace de datos.
    - Ethernet cableada.
    - Ethernet inalámbrica (otro tema).
    - Punto a punto.

Índice

Índice

Introducción a la capa de enlace de datos

- Términos:
  - **Nodos**: hosts y routers.
  - **Enlaces**: canales de comunicación que conectan nodos adyacentes a lo largo de la ruta:
    - Enlaces tecnología *cableada*.
    - Enlaces tecnología *inalámbrica*.
  - Capa de enlace de datos: responsable de encapsular el datagrama en una trama y transferirla desde un nodo emisor al nodo receptor adyacente a través de un *único enlace*.



Introducción a la capa de enlace de datos

- Un datagrama puede ser transferido por distintos protocolos de la capa de enlace (medios de transporte):
  - Ethernet. (Tren).
  - Punto a punto: Frame Relay. (Avión)
  - Wifi 802.11. (Autobús).
- Cada protocolo proporciona distintos servicios.
  - Mejor esfuerzo.
  - Entrega fiable.
- Unidad de datos de la capa de enlace: trama/frame (turista): encapsulación de los datagramas.
- Algoritmo de enrutamiento (agencia de viajes).

Servicios de la capa de enlace de datos

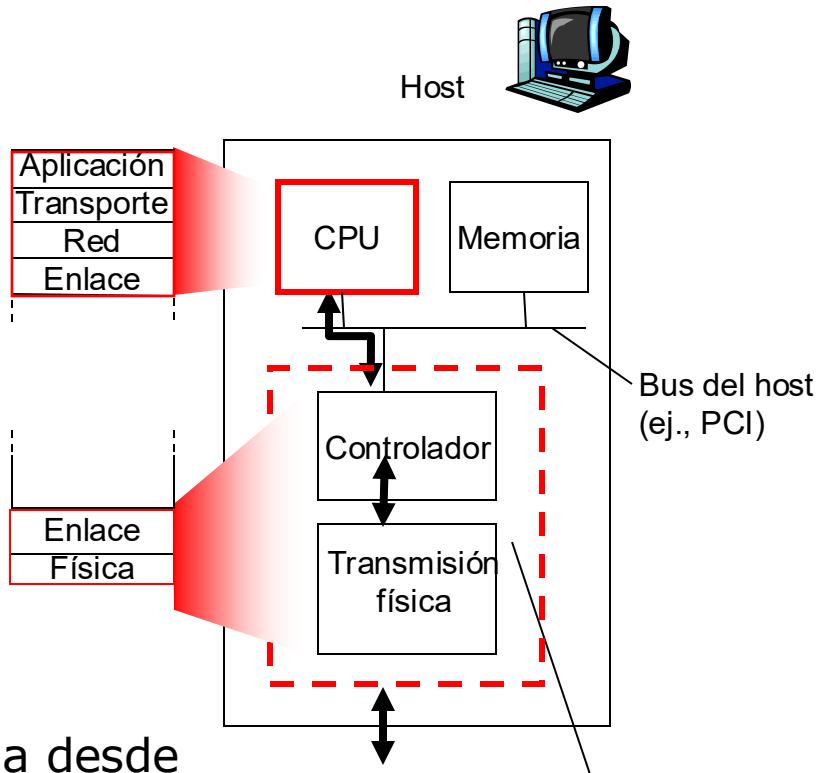
- Entramado.
  - Encapsulación de un datagrama en una trama, añadiendo cabecera y cola.
- Acceso al medio.
  - Reglas para transferir una trama a través del único enlace.
    - Sencillo en PPP.
    - Complejo en Ethernet (varios nodos compartiendo un mismo enlace de difusión): acceso múltiple.
- Entrega fiable.
  - Garantiza que se va a transportar cada datagrama de la capa de red a través del enlace sin producirse errores. Sobrecarga innecesaria, servicio no proporcionado. Proporcionado en Wifi 802.11.

Servicios de la capa de enlace de datos

- Control de flujo.
  - Los nodos extremos del enlace poseen capacidad limitada de almacenamiento en buffers. Problema: receptor no puede recibir tramas a más velocidad de la que puede procesarlas. Desbordamiento de buffer y pérdidas de tramas.
- Detección de errores.
  - Se producen errores de bits con atenuación de señales y ruido electromagnético. Solución: emisor añade bits de detección de errores en la trama. CRC vía hardware.
- Corrección de errores.
  - Emisor añade bits de corrección de errores a la trama.

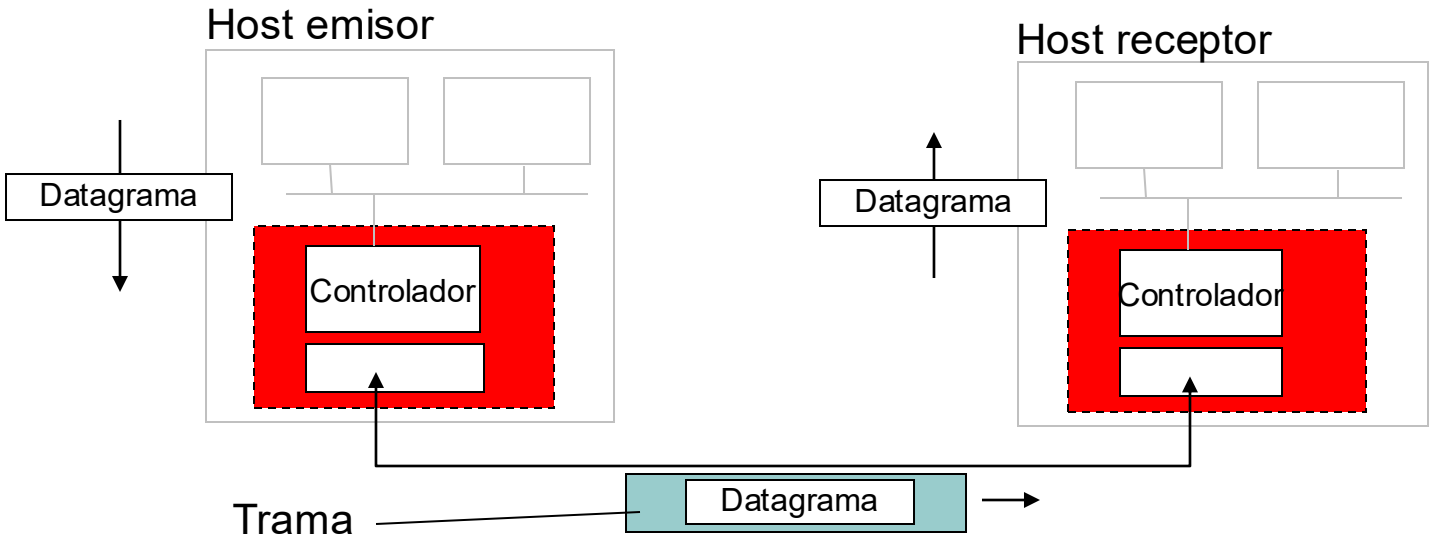
¿Dónde se implementa la capa de enlace?

- Implementación de la capa de red en cada host:
  - Adaptador de red, NIC
  - Tarjeta interface de red
    - PCI, PCI Express.
    - PCMCIA
    - Integrada en placa
  - Capas física y enlace.
  - Firmware del chip controlador.
  - Hardware:
    - Intel 8254x
    - Atheros.
  - Software:
    - Recepción del datagrama desde la capa de red
    - Entramado.
    - Activación de la IRQ de la NIC.



¿Dónde se implementa la capa de enlace?

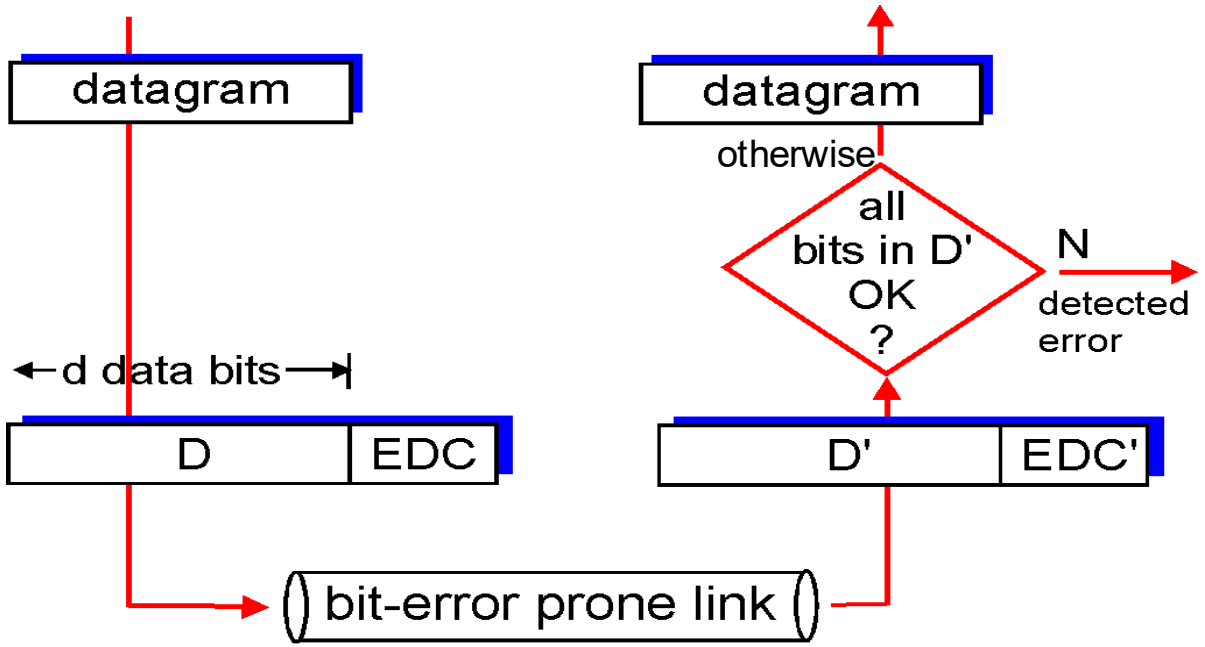
- Host **emisor**.
  - Encapsula datagrama en la trama.
  - Añade campos de cabecera.
  - Transmisión de la trama.
- Host **receptor**.
  - Recepción de la trama.
  - Analiza los campos de cabecera. Si procede detección de errores.



Índice

Técnicas de detección y corrección

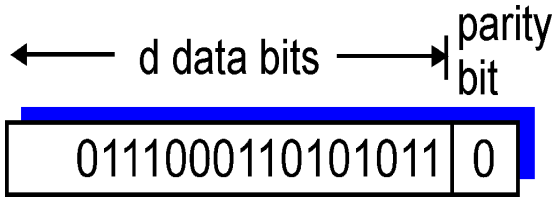
- EDC: Error Detection and Correction.
  - Bits EDC.
  - D: Datos transmitidos por emisor.
  - D': Datos recibidos en receptor.
  - ¿D'=D?
- Incluso utilizando bits de detección de errores pueden seguir existiendo errores de bit no detectados.



Comprobación de paridad

Bit de paridad par:

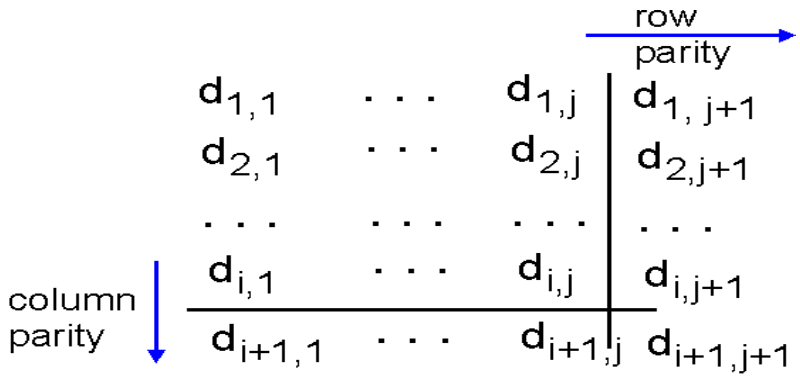
Detecta errores de un único bit

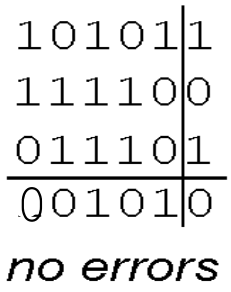


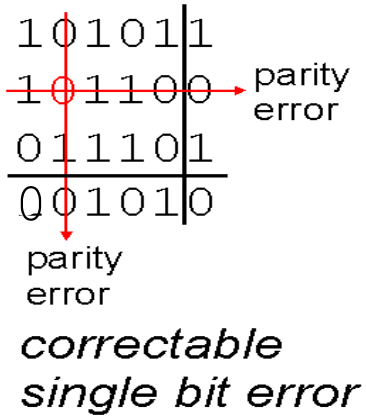
- FEC: Forward Error Correction.
- Reducen las retransmisiones de la capa de transporte.

Paridad par bidimensional:

Detecta and corrige un único bit







Comprobación de paridad

- Comprobación de paridad con 1 bit.
  - Sólo detecta errores de un bit; 3 bits; 5 bits. No detecta errores de un número de bits par.
    - Hipótesis válida (no real) si la P(error bit) es baja. Y los errores en bits del mismo paquete son sucesos independientes.
    - Realidad: los errores se acumulan por ráfagas en paquetes contiguos. Ráfagas de error. La P(errores no detectados) con comprobación de 1 bit de paridad es 50%.
- FEC: usado en unidades de CD audio además de capa de enlace de red.
  - Detectan y corrigen errores de 1 bit.
    - Corrige el receptor y no se necesita retransmisión.
  - Detectan errores de 2 bits.

Suma de comprobación (checksum)

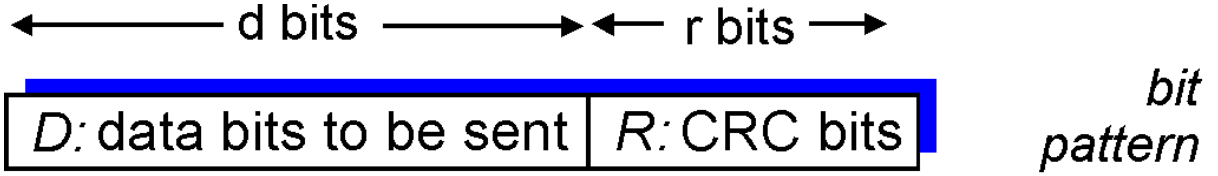
- Los ‘d’ bits de datos se tratan como una secuencia de enteros de ‘k’ bits.
  - Operación: sumar los enteros de ‘k’ bits.
    - El resultado: suma de comprobación.
- Suma de comprobación en Internet (RFC1071): ‘k’ = 16 bits.
  - Emisor:
    - Sumar palabras de 16 bits.
    - Suma de comprobación = el complemento a 1.
  - Receptor:
    - Sumar palabras de 16 bits (con checksum).
    - Suma de comprobación = el complemento a 1.
    - HFFFF => No hay error
    - Algún cero => hay error.

Suma de comprobación (checksum)

- Resumen de suma de comprobación en TCP/IP:
  - En capa 4 (TCP,UDP) se calcula sobre el segmento completo.
  - En capa 3 (IP) se calcula sobre la cabecera del datagrama.
- Suma de comprobación: software (propio S.O.).
- Capa de enlace se aplica cálculo CRC en hardware.

Suma de comprobación cíclica (CRC)

- CRC: Cyclic Redundancy Check.
- Códigos CRC: códigos polinómicos.
  - Polinomios con coeficientes 0 o 1: representan la cadena de bits.
- Considerar:
  - Secuencia **D** de datos con 'd' bits.
  - Emisor y receptor acuerdan patrón de 'r+1' bits: generador **G.**
    - Condición: bit más significativo de G = 1.
  - Objetivo: emisor selecciona 'r' bits a añadir a D.



$D * 2^r \quad XOR \quad R$ — *mathematical formula*

Suma de comprobación cíclica (CRC)

- Objetivo: el conjunto de <R,D> (en binario) debe ser exactamente divisible por G (resto nulo en aritmética módulo 2).
  - El receptor debe dividir los 'd+r' bits recibidos por G.
    - Si el resto es distinto de cero => receptor detecta error.
    - Si el resto = 0 => receptor detecta datos OK.
- Repaso aritmética módulo 2.
  - Cálculos CRC se realizan en aritmética módulo 2 sin acarreo en sumas ni restas.
  - Equivale a realizar operaciones XOR.
    - 1011 XOR 0101 = 1110
    - 1001 XOR 1101 = 0100
    - 1011 – 0101 = 1110
    - 1002 – 1101 = 0100.
  - Multiplicación y división iguales que en aritmética en base 2 (con sumas y restas XOR).
  - Multiplicación 2^k ⇔ desplazar 'k' posiciones a la izquierda.

Suma de comprobación cíclica (CRC)

Objetivo:

$$D \cdot 2^r \text{ XOR } R = nG$$

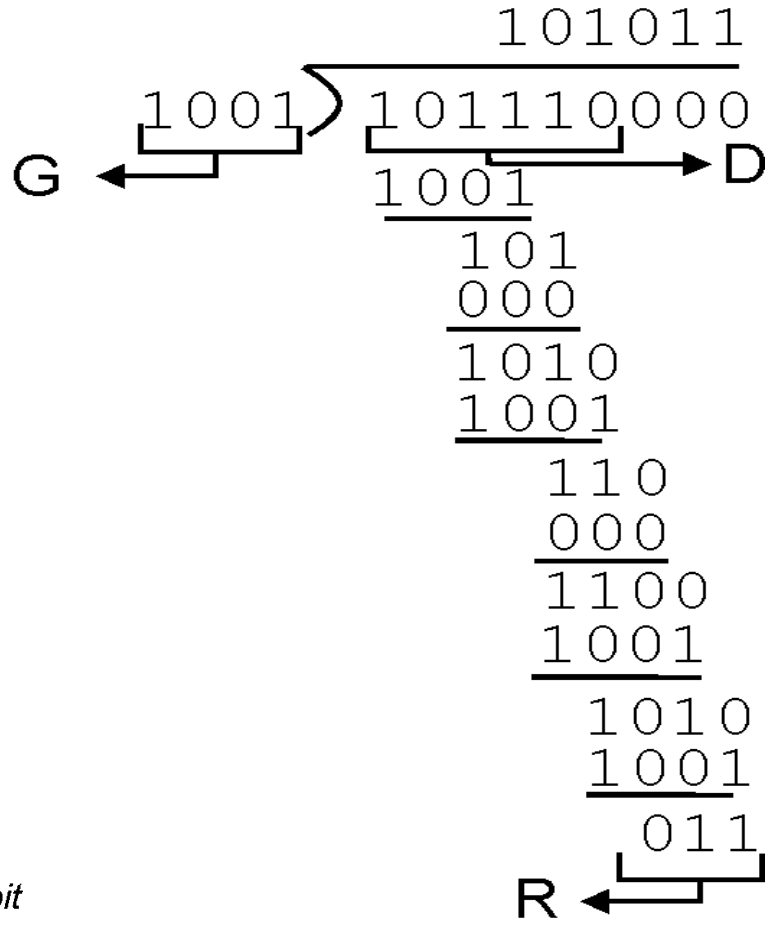
Equivale a:

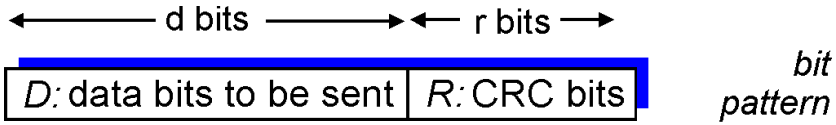
$$D \cdot 2^r = nG \text{ XOR } R$$

O equivale a:

Si dividimos $D \cdot 2^r$ por G, quiero obtener resto R

$$R = \text{Resto}\left(\frac{D \cdot 2^r}{G}\right)$$





bit pattern

$D * 2^r$ XOR R

mathematical formula

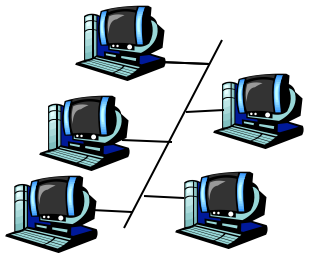
Suma de comprobación cíclica (CRC)

- Existen generadores de CRC para:
  - 8 bits (CRC-8): 0xD5
  - 12 bits (CRC-12): 0x80F
  - 16 bits (CRC-16): 0x8085
  - 32 bits (CRC-32): 0x40C11DB7.
- http://en.wikipedia.org/wiki/Cyclic_redundancy_check
- Los estándares CRC pueden detectar ráfagas de errores inferiores a r+1 bits (se detectan errores de r bits).
- Una ráfaga de longitud superior a 'r+1' bits será detectada con una probabilidad de: $1-0.5^r$.

Índice

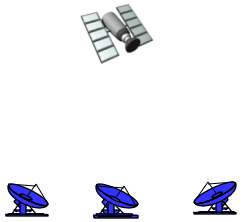
Protocolos de acceso múltiple

- 2 tipos de enlaces de red:
  - Enlace punto a punto (1 emisor y 1 receptor).
    - Protocolos de capa de enlace: PPP, HDLC.
  - Enlace de difusión: múltiples nodos emisores y receptores en un único canal.
    - Protocolos: Ethernet, LAN inalámbricas.
- Problema de acceso múltiple: como controlar el acceso de múltiples nodos emisores y receptores a un único canal de difusión compartido.
- Otros ejemplos de difusión: TV, radio.
  - Comparativa con una reunión de personas.



Cable compartido (Ethernet)

Señal RF (802.11 WiFi)



Señal RF (satélite)

Reunión social

Protocolos de acceso múltiple

- En un canal único multiacceso se necesita reglas/protocolo:
  - Protocolo de acceso múltiple: controla el acceso de los nodos (emisores/receptores).
  - Todos los nodos son capaces de transmitir tramas. Esto provocará **colisiones entre las tramas** en todos los nodos receptores.
    - Los receptores no son capaces de interpretar las tramas (tramas entremezcladas).
      - Tramas perdidas.
      - Pérdida de eficiencia (tiempo) del canal.
  - El protocolo debe coordinar las transmisiones.

Protocolos de acceso múltiple

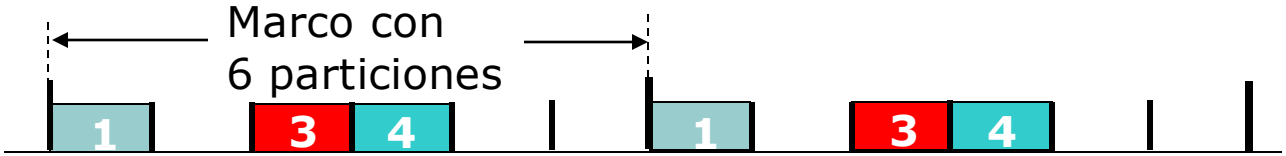
- Categorías de protocolos:
  - Protocolos de particionamiento del canal.
  - Protocolos de acceso aleatorio.
  - Protocolos de toma de turnos.
- Características de un protocolo ideal de acceso múltiples para un canal broadcast de R bps:
  - Cuando un nodo quiere transmitir, lo debería poder realizar a R bps.
  - Cuando N nodos quieren transmitir, cada uno dispondría de media R/N bps.
  - Será descentralizado: no habrá un único nodo maestro encargado del control (no supeditar al fallo del nodo maestro). Sin sincronización.
  - Simple de implementar.

Protocolos de particionamiento de canal

- Se particiona el canal en pequeños trozos (t,f).
- Cada trozo del canal se asocia a un nodo (uso exclusivo).
- Tipos:
  - TDM (Time Division Multiplexing).
  - FDM (Frecuency Division Multiplexing).
  - CDMA (Code Division Multiplexing Access).

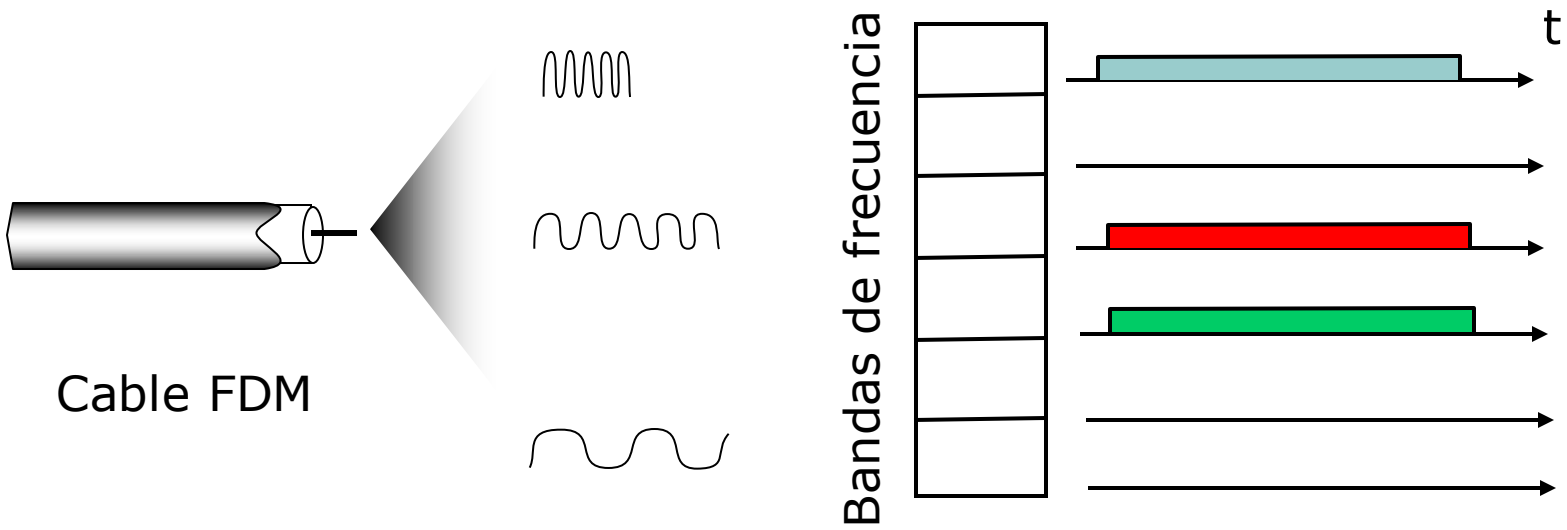
Protocolo TDM

- Multiplexación por división del tiempo.
  - El tiempo se divide en **marcos** temporales.
  - Cada marco temporal se subdivide en **particiones** de tiempo (time frame).
    - Cada partición se asigna a un nodo (N).
    - El tamaño de la partición suficiente (en tiempo) para transferir 1 trama.
    - Protocolo atractivo:
      - Elimina las colisiones.
      - Equitativo (R/N bps).
    - Desventajas:
      - Limitación de BW = R/N (para cada nodo).
      - Muy deficiente si muchos nodos no transmiten.



Protocolo FDM

- Multiplexación por división de la frecuencia.
  - Se divide el canal de R bps en diferentes **bandas de frecuencias** (cada una con un BW de R/N).
  - Posee las mismas ventajas e inconvenientes que TDM



Protocolo CDMA

- Acceso múltiple por división de código.
  - Se asigna un código único a cada nodo.
  - Cada nodo utiliza dicho código para codificar la trama a enviar.
  - Permite transmisión simultánea de muchos nodos.
  - Los receptores decodifican utilizando el código.
  - Uso militar y civil.
  - Buena inmunidad.
  - Uso en canales inalámbricos y telefonía celular.

Protocolos de acceso aleatorio

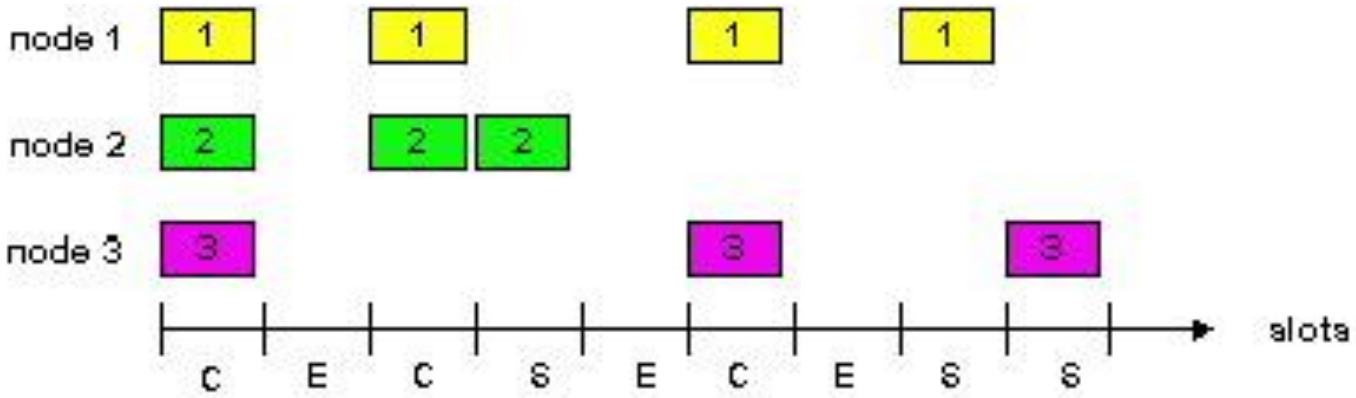
- Todos los nodos pueden tener acceso controlado (aleatorio) al canal.
- Cada nodo transmisor emite a la máxima velocidad del canal: R bps.
- Cuando se produce una colisión, los nodos implicados retransmiten repetidamente la trama hasta conseguir que lleguen al receptor.
  - **Espera durante un tiempo aleatorio antes de retransmitir la trama.**
  - Cada nodo independientemente selecciona un tiempo de retardo aleatorio
  - Seguro que un nodo habrá seleccionado un retardo menor que el resto y conseguirá retransmitir la trama con éxito (sin colisión).
- Ejemplos: Aloha con particiones, Aloha puro, CSMA.

Protocolo Aloha con particiones

- Hipótesis:
  - Todas las tramas tienen **L** bits.
  - El tiempo está dividido en particiones de **L/R** s. Cada partición equivale al tiempo de transmisión de una trama.
  - Los nodos comienzan a transmitir las tramas sólo al principio de las particiones.
  - Los nodos están sincronizados (reloj). Cada nodo sabe cuándo comienzan las particiones.
  - Si 2 o más tramas colisionan en una partición, todos los nodos detectan la colisión, incluso antes de que finalice la partición.
- Funcionamiento:
  - Si un nodo quiere enviar una trama, espera hasta el comienzo de la siguiente partición y la envía.
  - Si **no hay colisión** (llegando el receptor), el nodo no considera retransmitirla. Se prepara para enviar otra trama.
  - Si **hay colisión**, el nodo detecta la colisión antes de que la partición finalice. El nodo **retransmitirá** su trama en cada partición posterior con una probabilidad **p**, hasta conseguirlo.

Protocolo Aloha con particiones

- Ventajas:
  - Cada nodo puede transmitir a **R** bps.
  - Descentralizado: cada nodo detecta las colisiones y decide individualmente cuándo retransmitir.
  - Simple
- Desventajas:
  - Requiere que las particiones estén sincronizadas.
  - Las colisiones provocan baja eficiencia del protocolo.
  - Hay particiones sin aprovechar (emitiendo). Probabilística.
  - Los nodos deben detectar las colisiones antes de finalizar la partición.



Protocolo Aloha con particiones

- Eficiencia: fracción de particiones con éxito (medida a largo plazo) cuando existen gran número de nodos activos.
  - Suponer **N nodos** con posibilidad de transmitir una trama en cada partición con **probabilidad p**.
  - Probabilidad de que un nodo transmita la trama con éxito:

$$\mathbf{p(1-p)^{N-1}}$$

  - Probabilidad de que cualquier nodo transmita la trama con éxito:

$$\mathbf{Np(1-p)^{N-1}}$$

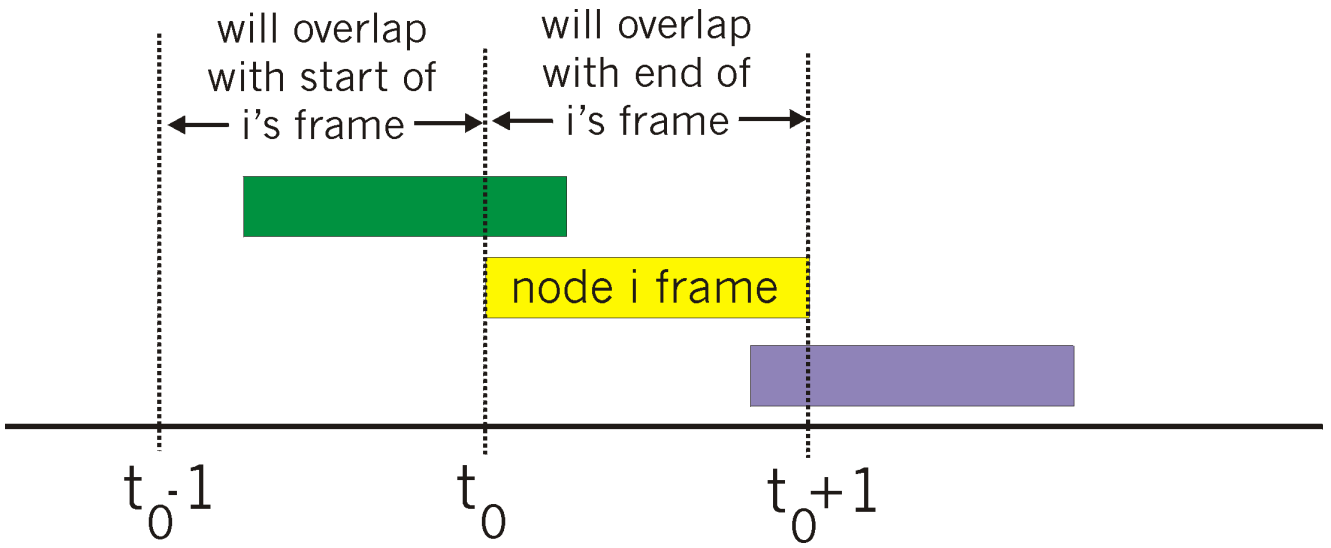
    - Máxima eficiencia: buscar p que maximice la función: $\mathbf{E(p)= Np(1-p)^{N-1}}$
    - Para un elevado número de nodos N calcular el límite donde N -> ∞ en:

$$\mathbf{E_{max}(p=1/N)= (1-1/N)^{N-1}}.$$

    - Máxima eficiencia E_{max}= 1/e= 0.37.
    - Uso máximo del canal = 37%.

Protocolo Aloha puro (sin particiones)

- Más simple, y no requiere sincronización.
- Cuando al nodo le llega una trama, la transmite hacia el canal de difusión.
- Aumenta la probabilidad de colisión:
  - La trama enviada puede colisionar con tramas de otros nodos enviadas en
    - $[t_0-1, t_0+1]$



Protocolo Aloha puro (sin particiones)

- Eficiencia: fracción de particiones con éxito (medida a largo plazo) cuando existen gran número de nodos activos.
  - Suponer **N nodos** con posibilidad de transmitir una trama en cada partición con **probabilidad p**.
  - Probabilidad de que un nodo transmita la trama con éxito:

    $$\mathbf{p(1-p)^{2(N-1)}}$$

  - Probabilidad de que cualquier nodo transmita la trama con éxito:

    $$\mathbf{Np(1-p)^{2(N-1)}}$$

    - Máxima eficiencia: buscar p que maximice la función: $\mathbf{E(p)= Np(1-p)^{2(N-1)}}$
    - Para un elevado número de nodos N calcular el límite donde N -> ∞ en:

      $$\mathbf{E_{max}(p=1/(2N-1))= [1-1/(2N-1)]^{2(N-1)}}.$$

    - Máxima eficiencia E_{max}= 1/2e= 0.18.
    - Uso máximo del canal = 18%.

Protocolo CSMA

- En Aloha los nodos deciden transmitir tramas independientemente de la actividad de envíos del resto de nodos.
  - No prestan atención si hay nodos transmitiendo.
  - Tampoco dejan de transmitir si otros nodos comienzan a enviar tramas.
- Solución: CSMA: Carrier Sense Multiple Access.
  - Reglas:
    - Escucha antes de hablar ⇔ **Sondeo de portadora**: cada nodo escucha el canal antes de transmitir.
      - Si el canal está siendo utilizado por otro nodo, se espera un tiempo aleatorio y luego se vuelve a sondear para ver si existe portadora en el canal.

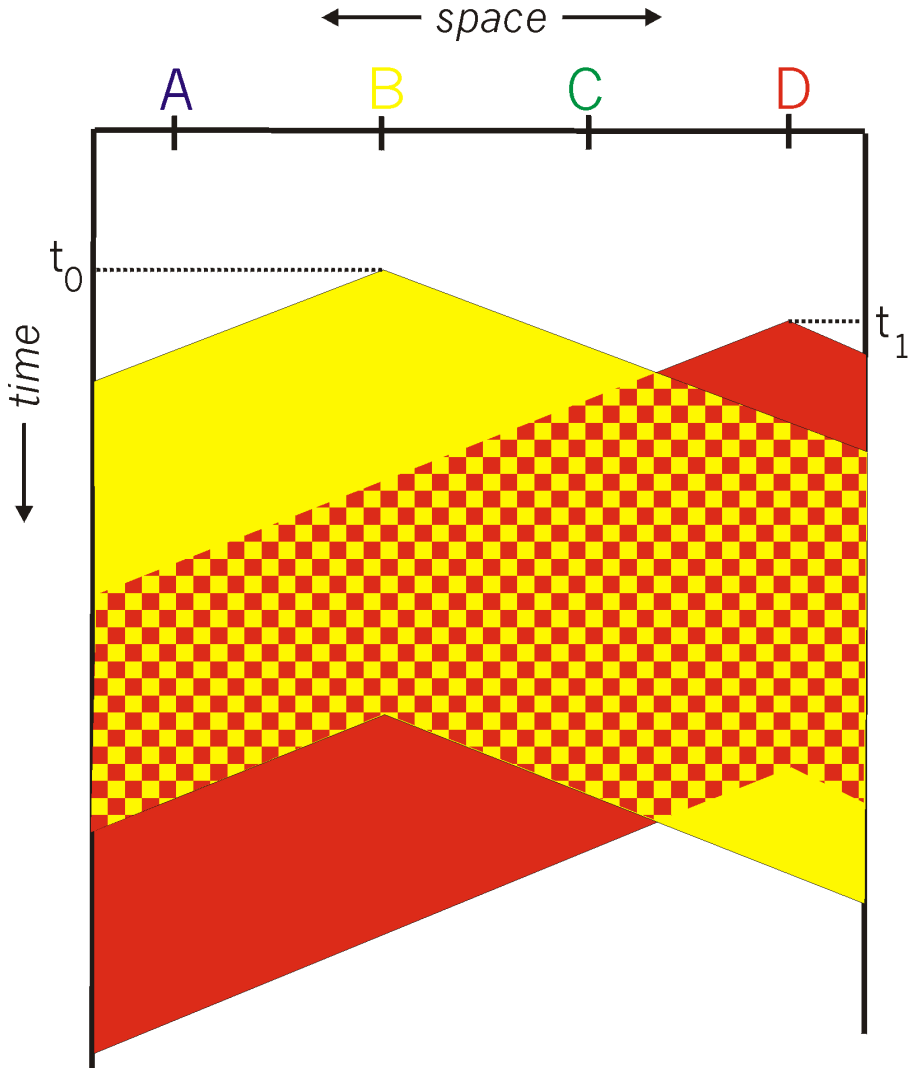
Protocolo CSMA

- Reglas:
  - Si alguien comienza a hablar al mismo tiempo, hay que dejar de hablar ⇔ **Detección de colisiones**: un nodo transmitiendo una trama escucha lo que hay en el canal mientras dura la transmisión.
    - Si detecta otro nodo transmitiendo una trama que interfiere con la suya, dejará de transmitir y seguirá reglas de protocolo para volver a intentar transmitir de nuevo.
  - Protocolos: CSMA y CSMA/CD (Ethernet).
- ¿Porqué hay colisiones aún aplicando Sondeo de portadora?
  - Analizar diagramas espacio-tiempo de evolución de tramas de nodos

Protocolo CSMA

- El retardo de propagación del canal, influye.
  - A mayor retardo propagación, mayor es la probabilidad de colisión.
- Instante t_0, nodo B comienza a transmitir a C y A.
- En t_1 ($t_1 > t_0$) a D no le ha llegado trama de B, y trasmite trama a C.
- Colisión de tramas.

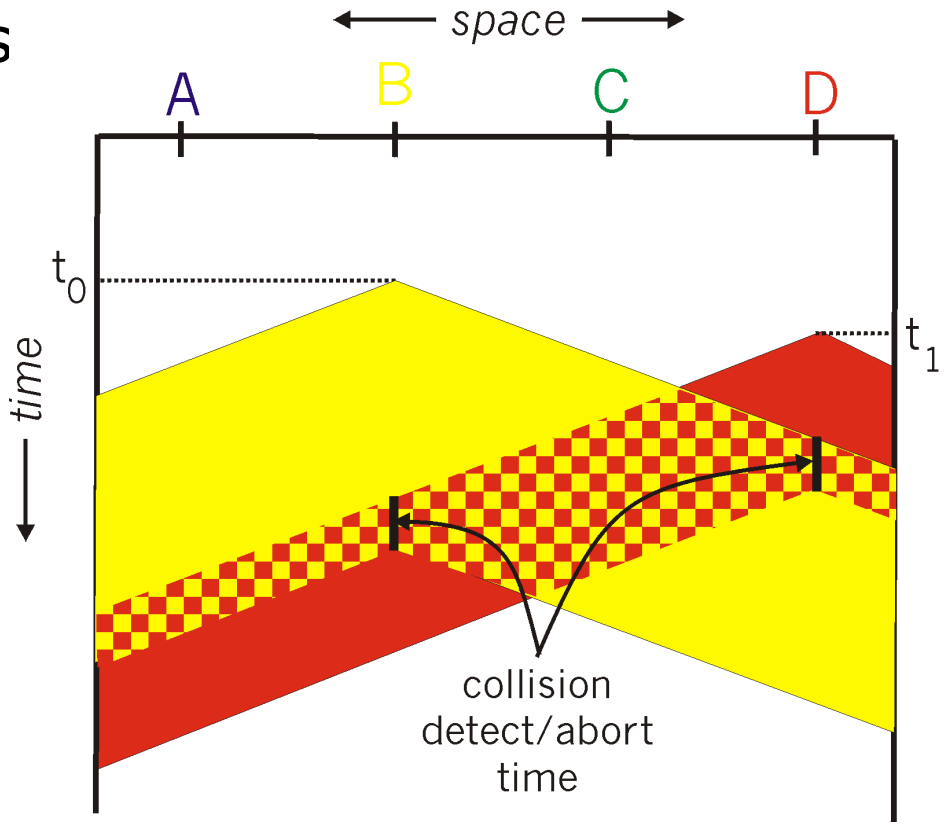
Diagrama espacio/tiempo de nodos



Protocolo CSMA

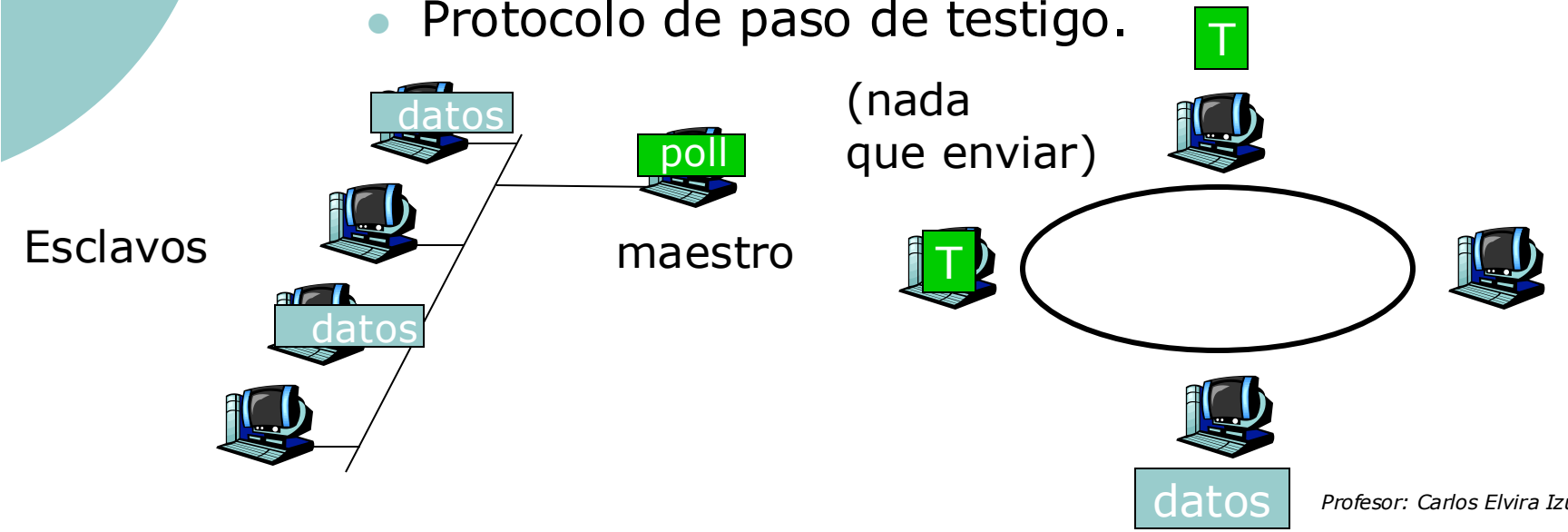
- Los nodos B y D anulan la transmisión de sus tramas un tiempo después de detectar la colisión.
- Ethernet utiliza CSMA con detección de colisiones.

Diagrama espacio/tiempo de nodos



Protocolos de toma de turnos

- Protocolo de acceso múltiple ideal:
  - Cuando sólo hay un nodo activo, éste dispone de R bps.
  - Cuando hay N nodos activos, cada nodo dispondrá de R/N bps.
- Aloha y CSMA cumplen la primera condición, pero no la segunda.
- Protocolos de toma de turnos tratan de cumplir las 2 condiciones:
  - Protocolo de sondeo (polling).
  - Protocolo de paso de testigo.



Protocolo de sondeo

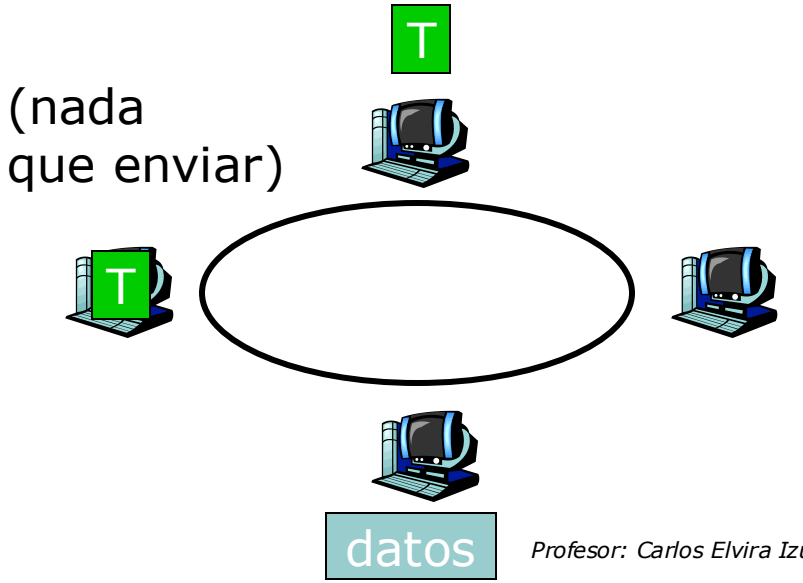
- Requiere un nodo maestro.
  - El nodo maestro sondea a cada uno del resto de nodos en un turno rotatorio (round robin):
    - Envía mensaje al nodo 1, invitándole a transmitir un número máximo de tramas.
    - Tras transmitir el nodo 1, el nodo maestro invitará al nodo 2 transmitir tramas.
  - Se eliminan las colisiones y las particiones vacías. Mayor eficiencia.
  - Desventajas:
    - Se introduce el retardo d_{sondeo}.
    - Si falla el nodo maestro, el canal no es operativo.
- Ejemplo: Bluetooth (802.15)

Protocolo de paso de testigo

- Un pequeña trama especial (testigo) se intercambia entre los nodos en un orden determinado.
  - El nodo 1 pasa el token el nodo 2.
  - El nodo 2 pasa el testigo al nodo 3.
  - …
- Cuando un nodo recibe el testigo, lo retiene si tiene tramas que enviar.
  - Envía hasta el máximo número de tramas permitido, y luego reenvía el token.
  - Caso de no tener tramas que enviar, reenvía el testigo al nodo siguiente.
- Protocolo descentralizado y eficiente.
- Problema: fallo de un nodo o retención del testigo en un nodo.
  - Procedimiento para reiniciar la circulación del testigo.
- Ejemplo: FDDI (802.5)

Protocolo 802.5 (FDDI)

- Protocolo FDDI (802.5): Fiber Distributed Data Interface.
  - Utilizada en MAN (Metropolitan Area Network).
  - FDDI hace que el nodo destino eliminela trama del anillo.
  - No circula por todo el anillo.
    - No es un canal de difusión puro.
      - No todos los nodos reciben las tramas transmitidas.



Índice

Direccionamiento en la capa de enlace

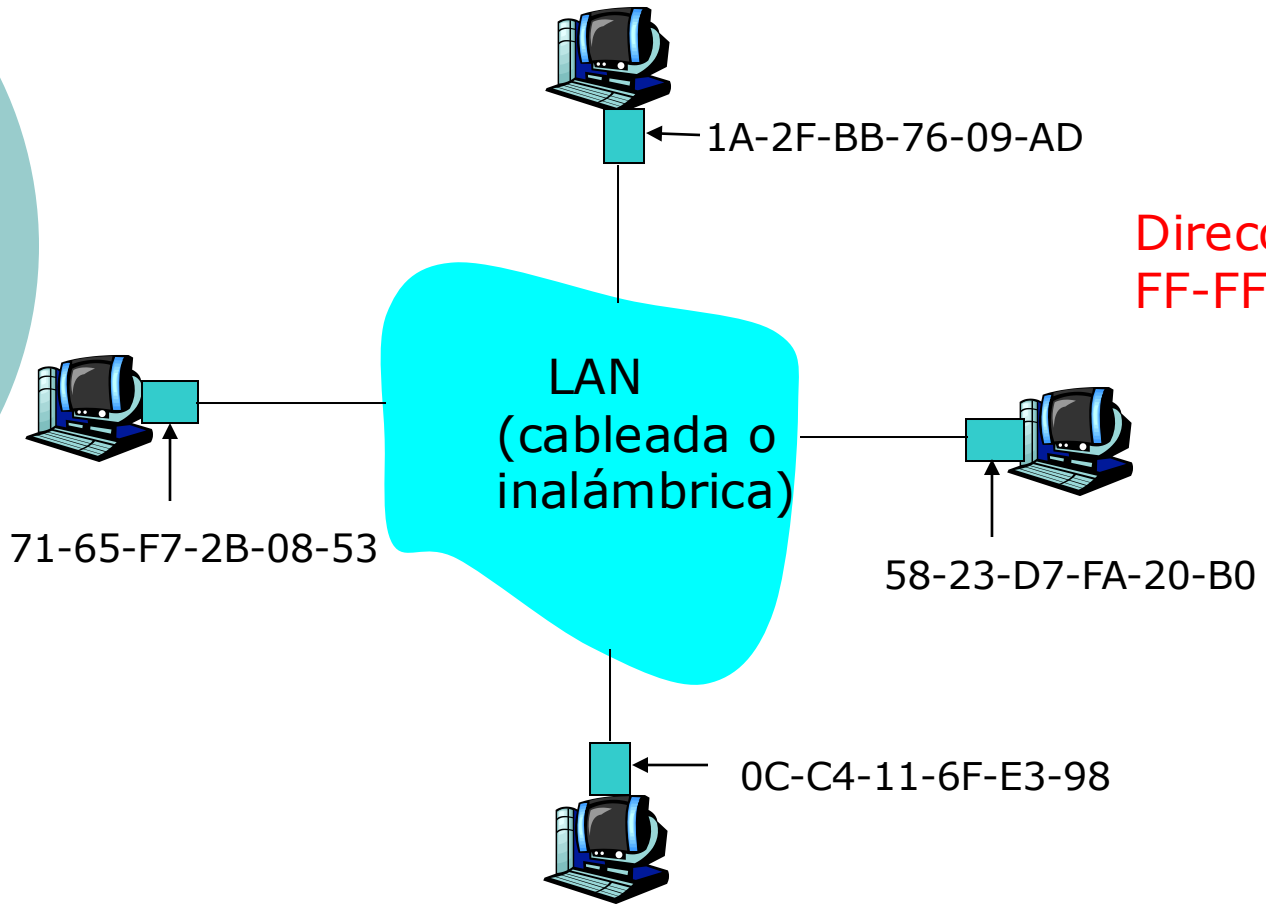
- Todos los nodos (hosts) posee direcciones de capa de enlace.
  - Además de dirección de capa de red IP.
  - Las direcciones se asignan a las tarjetas instaladas en cada nodo.
  - Direcciones de capa de enlace, LAN, física o MAC:
    - 6 bytes = 48 bits.
      - 2^{48} posibles direcciones MAC.
      - 24 bits OUI (Organisationally Unique Identifier)
      - 24 bits NIC (Network Interface Controller) Specific
      - Dirección MAC única.
        - Se pueden cambiar vía software.
    - Codificación hexadecimal: 12:34:56:78:9a:bc.
    - 24 bits asignados por IEEE a la empresa.
    - 24 bits de menor peso para identificar cada tarjeta.
    - Estructura plana (dirección IP posee estructura jerárquica)

Direccionamiento en la capa de enlace

- Permite enviar una trama desde un nodo origen al otro nodo extremo final del cable físico.
  - El nodo emisor inserta MAC de destino en la trama.
  - Cada adaptador que recibe la trama comprueba si existe coincidencia con la dirección MAC destino.
  - Si existe coincidencia en la MAC, el adaptador extrae el datagrama de la trama y lo envía a la capa 4.
- Un emisor puede enviar tramas al resto de nodos con dirección MAC de difusión:
  - MAC broadcast: ff:ff:ff:ff:ff:ff

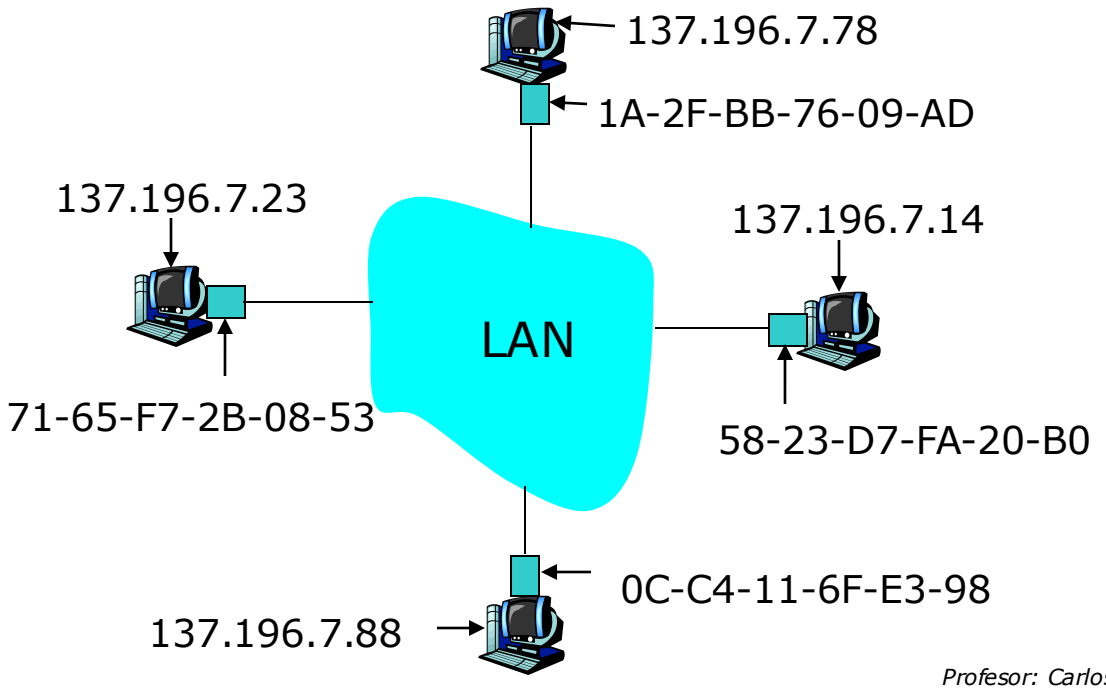
Direccionamiento en la capa de enlace

Cada tarjeta en una LAN posee una dirección MAC única



Protocolo ARP

- ARP: Address Resolution Protocol.
- RFC 826.
- Permite obtener la MAC a partir de su dirección IP.
- Cada nodo (host, router) en una LAN posee una tabla ARP



Protocolo ARP

Internet Protocol (IPv4) over Ethernet ARP packet		
octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

Protocolo ARP

- Estructura en C con paquete ARP.
  - Notación: little-endian.

```
struct arp

{

   u16 htype; // Hardware type

   u16 ptype; // Protocol type

   u8  hlen; // Hardware address length (Ethernet = 6)

   u8  plen; // Protocol address length (IPv4 = 4)

   u16 opcode; // ARP Operation Code
   u8  srchw[hlen]; // Source hardware address - hlen bytes (see
above)
   u8  srcpr[plen]; // Source protocol address - plen bytes (see
```

Protocolo ARP

- Formato del paquete: 28 bytes.
  - HTYPE: Tipo de protocolo encapsulado como carga de datos en una trama Ethernet.
  - PTYPE: Protocolo de capa de red que solicita ARP.
    - EtherType: http://en.wikipedia.org/wiki/EtherType
  - HLEN: Longitud (bytes) de la dirección física.
  - PLEN: Longitud de la dirección de capa de superior (red).
  - Operación: solicitud (1), respuesta (2).
  - SHA: dirección MAC del emisor.
  - SPA: dirección de red del emisor.
  - THA: dirección MAC del receptor.
  - TPA: dirección de red del receptor.

Protocolo ARP

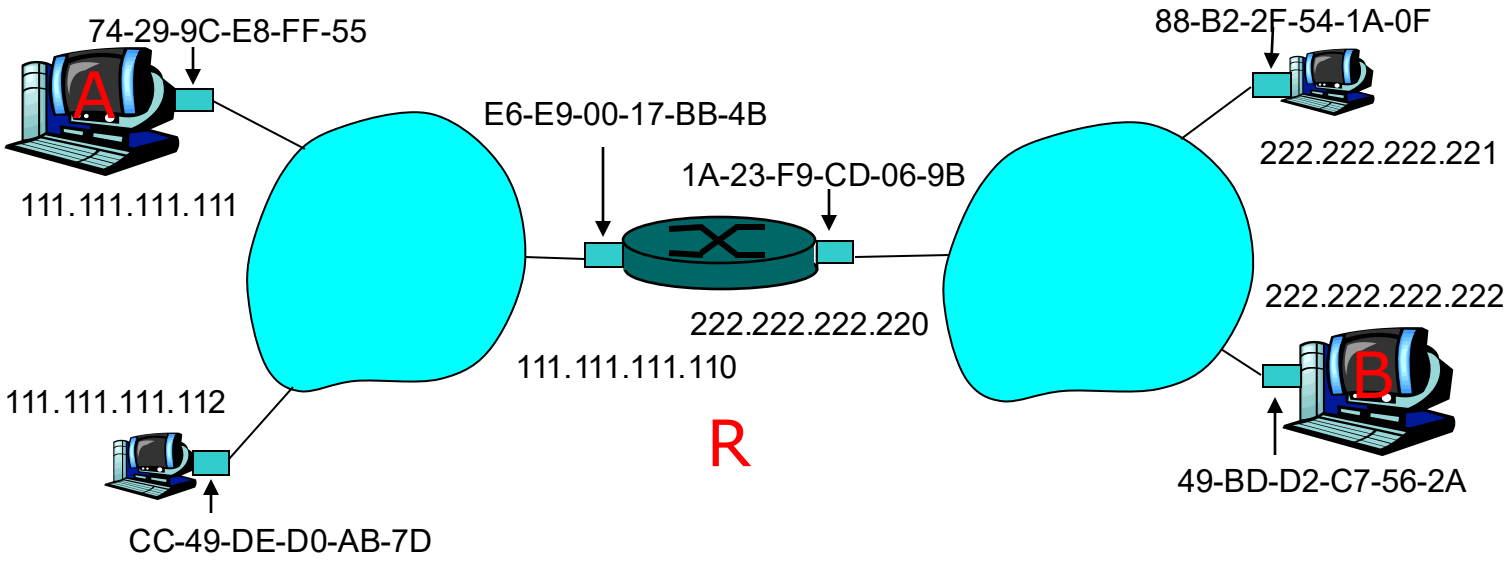
- Tabla ARP: mapea direcciones IP/MAC en todos los nodos de la LAN.
  - Entrada: < dirección IP; dirección MAC; TTL>
  - TTL (Time To Live): tiempo que permanece la entrada en la tabla ARP (20 min). En PC linux 60s.
    - cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
    - sysctl –a | grep gc_stale_time
- Funcionamiento:
  - Nodo A (78) quiere enviar datagrama a nodo B (88).
  - A no conoce la MAC de B: 0C-C4-11-6F-E3-98.
  - A envía una consulta ARP tipo broadcast a todos los nodos del canal (vía ff:ff:ff:ff:ff:ff).
  - Todos los nodos reciben la consulta broadcast. Nodo B la recibe y responde al nodo A con su MAC.
    - La respuesta de B al nodo A es unicast.

Protocolo ARP

- Funcionamiento:
  - Los paquetes consulta/respuesta ARP posee el mismo formato.
  - El nodo A guarda la entrada en la tabla hasta que caduque
  - ARP es un protocolo plug and play: la tabla ARP de cada nodo se construye automáticamente (no es configurada por el administrador de sistemas).
- ARP es un protocolo de capa 2 o 3?
  - Un paquete ARP se encapsula dentro de una trama de la capa de enlace. Se sitúa por encima de la capa de enlace.
  - Un paquete ARP dispone de campos que contienen direcciones MAC. Se sitúa como protocolo de la capa de red

Protocolo ARP

- Protocolo ARP en los interfaces de un router:
  - 2 tablas ARP en el router. Una para cada interface.
  - Nodo A envía la trama con ¿MAC destino? Aprendida vía ARP en la interface izquierda.
  - El router modifica la IP al pasar a la subred derecha.
  - La interface derecha del router aprende MAC del nodo B vía ARP.



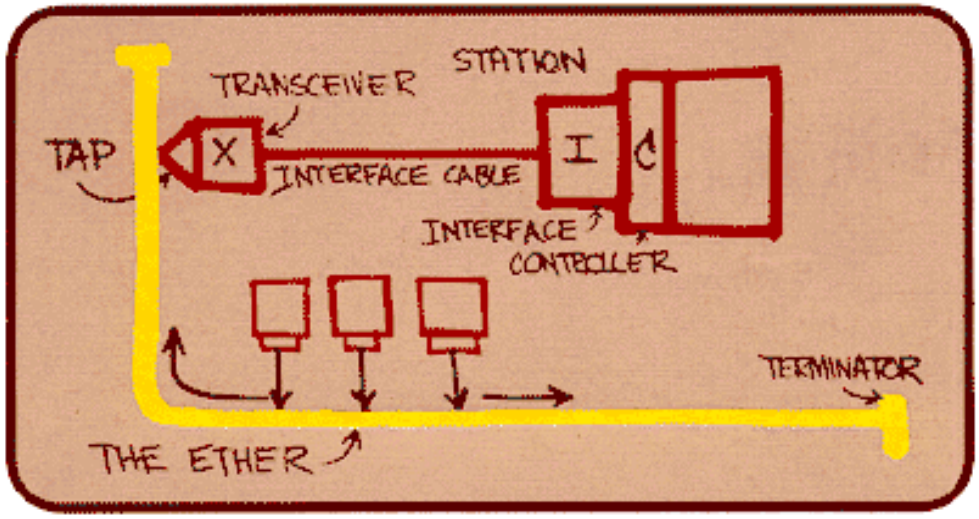
Índice

Ethernet

- Tecnología de capa 2 y 1 aplicada a LANs.
  - Otras tecnologías: ATM, FDDI, Token Ring.
- Orígenes: 1970 Bob Metcalfe. Mejora la idea de la red de Aloha aplicando las 2 ideas de CSMA/DC:
  - Antes de transmitir cada nodo sondea la señal portadora ¿canal libre?.
  - Mientras transmite el nodo escucha el canal ¿detecta colisión?.
- Junto con David Boggs se contruyó la red.
- Topología de bus.
- Bus coaxial.

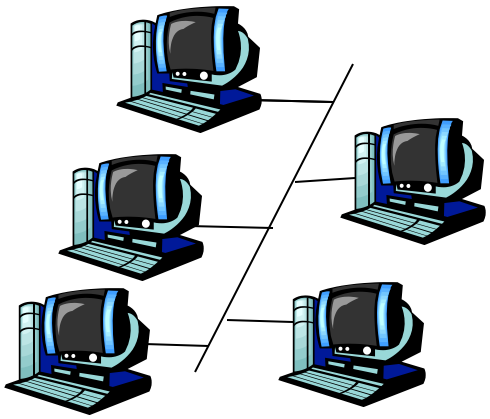
Ethernet

- Velocidad 2.94 Mbps.
- Cable coaxial de 50 Ohm.
- Segmento de cable de 1.6 km.
- Direcciones de 8 bits.
- CRC de 16 bits.
- Propiedad de XEROX PARC.

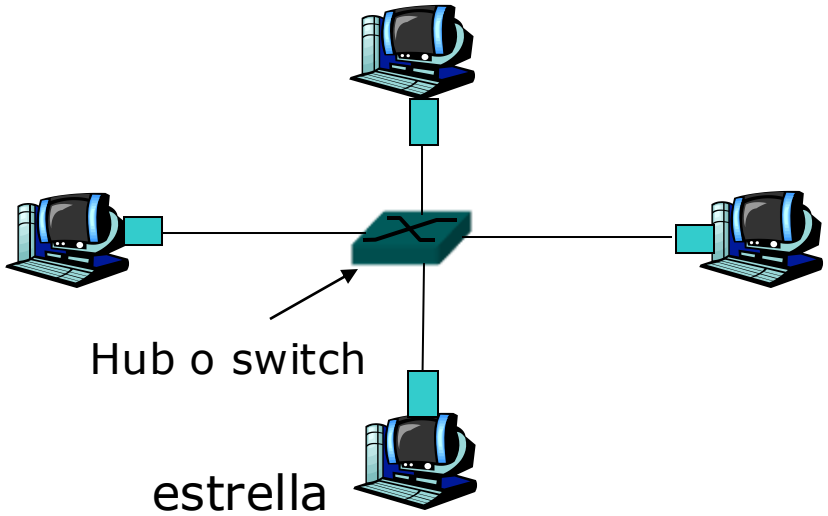


Ethernet

- Década de los 80 y mediados de los 90: topología de bus.
- Finales de los 90: topologías en estrella con concentradores.
  - Los hosts se conectan al hub mediante cable par trenzado (dominio de colisión)
    - El concentrador (capa física) regenera los bits.



bus: cable coaxial



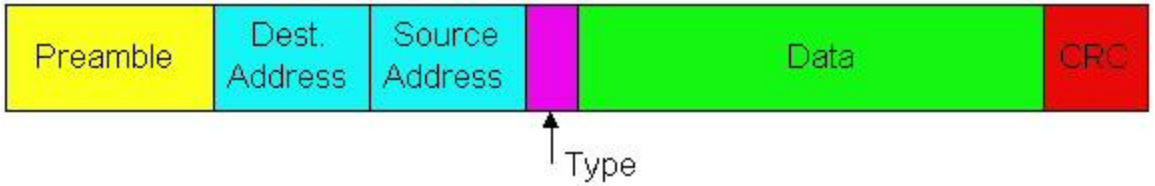
estrella

Ethernet

- Principio de la década de 2000: sustitución del hub por switch.
  - Conmutador que evita colisiones operando inteligentemente en la capa 2.

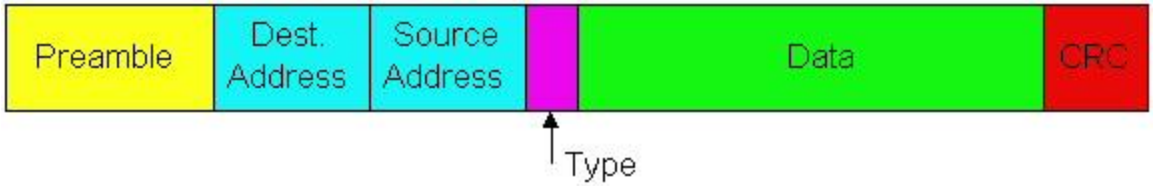
Estructura de la trama de Ethernet

- La carga útil de una trama es un datagrama IP (o de otro tipo de capa de red).
  - El emisor encapsula datagrama dentro de trama Ethernet añadiendo.
    - Cabecera.
    - Cola.
  - Pasa la trama a capa física y transmite los bits.
  - El receptor recibe la trama. Extrae el datagrama IP y lo pasa a capa de red



Estructura de la trama de Ethernet

- Campos de la cabecera:
  - Preámbulo (8 bytes). 7 bytes 10101010B y el último byte 10101011B.
    - Despiertan a las tarjetas de red y sincronizan relojes con el emisor (anular la deriva de la velocidad de transmisión teórica).
  - Dirección MAC destino. 6 bytes.
  - Dirección MAC origen. 6 bytes.
  - Tipo (EtherType). 2 bytes. Indica el protocolo de capa de red utilizado.
    - EtherType: http://en.wikipedia.org/wiki/EtherType
  - Datos: (46 a 1500 bytes = MTU)
  - CRC. 4 bytes.



Servicios de Ethernet

- Servicio sin conexión: no proporciona conexión a la capa de red.
  - Cuando el adaptador dese enviar un datagrama el otro extremo, encapsula el datagrama y lo envía a la LAN. Equivale a UDP (capa 4).
- Servicio no fiable a la capa de red. No existe reconocimiento de llegada ni tampoco reconocimiento de fallo en CRC.
  - El flujo de datagramas pasado a capa de red puede contener huecos (tramas descartadas)
  - La fiabilidad se deja a capa 4.
- Ethernet es simple y tecnología barata.

Protocolo CSMA/CD de Ethernet

- LAN Ethernet es una LAN de difusión (broadcast).
  - Necesita protocolo de acceso múltiple: CSMA/CD.
    - Un adaptador puede comenzar a transmitir en cualquier instante. No existe partición de tiempo.
    - Un adaptador nunca transmite una trama cuando detecta que otro adaptador está transmitiendo. Utiliza **sondeo de portadora**.
    - Un adaptador que está transmitiendo aborta su transmisión tan pronto como detecta que otro adaptador también transmite. Mecanismo de **detección de colisiones**.
    - Antes de intentar una retransmisión, un adaptador espera un intervalo de tiempo aleatorio, que normalmente es más pequeño que el tiempo que se tarda en transmitir una trama.

Protocolo CSMA/CD de Ethernet

- CSMA/CD posee un rendimiento mucho mayor que Aloha con particiones.
  - Si $d_{propagación}$ es muy pequeño => eficiencia tiene al 100%.
- Para detectar si otra tarjeta transmite, y para detectar colisiones mientras transmite, las tarjetas Ethernet miden niveles de tensión antes y durante las transmisiones.

Protocolo CSMA/CD de Ethernet

- Funcionamiento del protocolo en un adaptador:
  - La tarjeta obtiene datagrama de la capa de red, prepara la trama Ethernet y la coloca en un buffer de la tarjeta.
  - Si la tarjeta detecta que el cana está inactivo….
    - Mira durante 96 t_{clk} que la tarjeta no recibe intensidad de señal del canal
  - … comienza a transmitir la trama. Si el adaptador detecta canal ocupado, espera hasta que no hay intensidad de señal en el canal (añade 96 t_{clk}) y comienza a transmitir.
  - Mientras está transmitiendo, la tarjeta analiza la señal del canal; comprueba que otras tarjetas emiten. Si otra tarjeta no emite...
    - La tarjeta finaliza la transmisión de la trama.
  - … Si se detecta señal de otra tarjeta, deja de transmitir y transmite señal de interferencia (jam) de 48 bits.
  - Aborta la transmisión de su trama y se entra es fase de espera exponencial (**backoff exponential**). La retransmisión tras la n-ésima colisión se realiza una selección de un valor aleatorio K.

Protocolo CSMA/CD de Ethernet

- La retransmisión tras la n-ésima colisión se realiza una **selección de un valor aleatorio K** del conjunto Ω:
  $\{0, 1, 2, \ldots, 2^m-1\}$ donde m=min(n,10).
- Tiempo de espera aleatorio: $t_{backoff}=K\ 512\ t_{clk}$.
- Se vuelve al comienzo.

- La señal de interferencia (jam) que todos los adaptadores que están transmitiendo sean conscientes de la colisión.
- Ejemplo: Ethernet 10 Mbps $t_{clk}=0.1\mu s$.
  - Un adaptador intenta transmitir trama por primera vez y mientras lo hace detecta colisión. => $K\in \Omega_1=\{0,1\}$
    - Probabilidad de seleccionar K=0 o K=1 (p=0.5).
    - Selecciona K=0 (p=0.5) => pasa trama inmediatamente.
    - Selecciona K=1 (p=0.5) => $t_{backoff}=51,2\mu s$.
  - Después de una segunda colisión: $K\in \Omega_2\{0,1,2,3\}$.
    - Probabilidad de seleccionar K=0, K=1, K=2 o K=3 (p=0.25).
  - Después de una tercera colisión: $K\in \Omega_3\{0,1,2,3,4,5,6,7\}$.
    - Probabilidad: p=0.125.
  - Después de 10 colisiones o más: $K\in \Omega_{10}\{0,1,\ldots,1023\}$.

Protocolo CSMA/CD de Ethernet

- Observar que el tamaño de los conjuntos Ω crece exponencialmente.
  - Algoritmo backoff exponencial.
- Justificación:
  - Inicialmente el adaptador no conoce el número de tarjetas existentes en el segmento compitiendo por el uso del canal.
  - Primero se asigna un asigna al conjunto Ω unos pocos valores presuponiendo que no hay muchas tarjetas.
  - Aumentando el tamaño del conjunto Ω después de cada colisión, las tarjetas implicadas en la colisión van asignando distintos valores consiguiendo alguna de ellas enviar su trama y evitar la colisión.
- Cada vez que un adaptador prepara una nueva trama a transmitir en el canal ejecuta CSMA/CD sin tener en cuenta las colisiones que han ocurrido en anteriores transmisiones.

Protocolo CSMA/CD. Eficiencia.

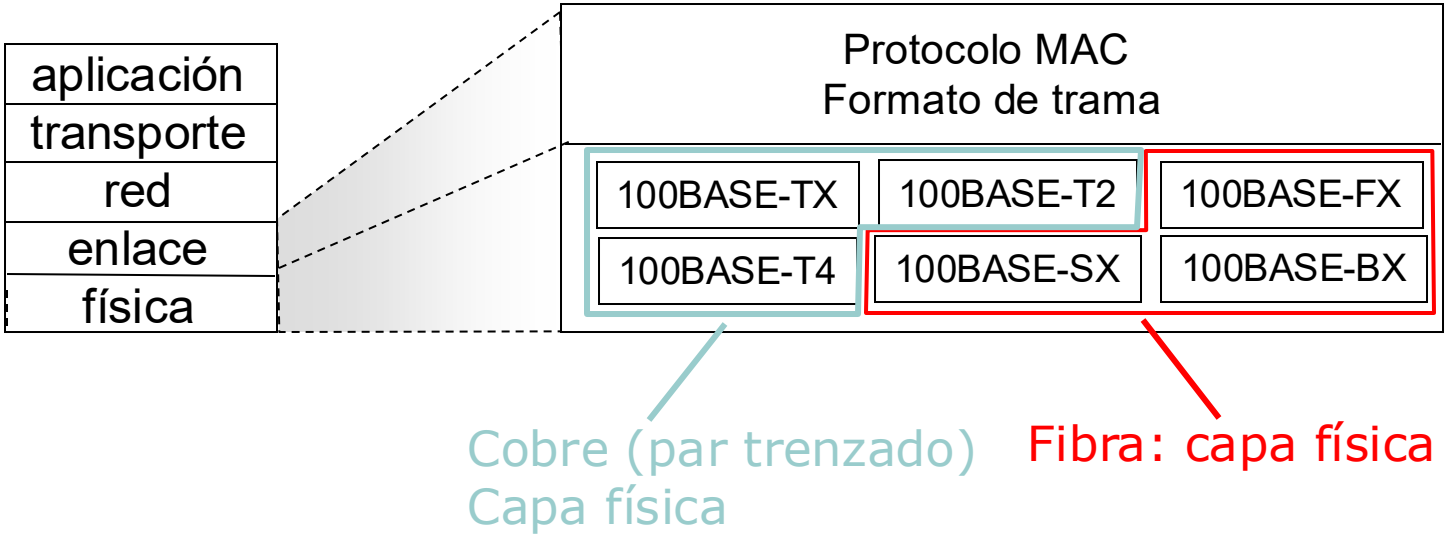
- Eficiencia de Ethernet: fracción (a largo plazo) de tiempo durante el que las tramas están siendo transmitidas al canal sin colisiones, cuando existe un gran número de tarjetas activas y cada una de ellas con una gran cantidad de tramas a enviar.

$$eficiencia = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

  - La eficiencia tiende a 1 cuando:
    - t_{prop} tiende a 0. Los nodos implicados en la colisión abortan transmisión. Se evita desperdicio de tiempo en el canal.
    - t_{trans} tiende a ∞. Una trama se apropia del canal mucho tiempo, transmitiendo eficientemente datos sin colisiones.

Tecnologías Ethernet.

- Ethernet posee su protocolo CSMA/CD.
- Ethernet es un conjunto de tecnologías (estándares) evolucionando constantemente bajo IEEE 802.3 CSMA/CD:
  - Posee un protocolo MAC común: CSMA/CD.
  - Poseen distintas velocidades: 2Mbps, 10Mbps, 100Mbps, 1Gbps, 10Gbps.
  - Distintos medios físicos: cobre, fibra



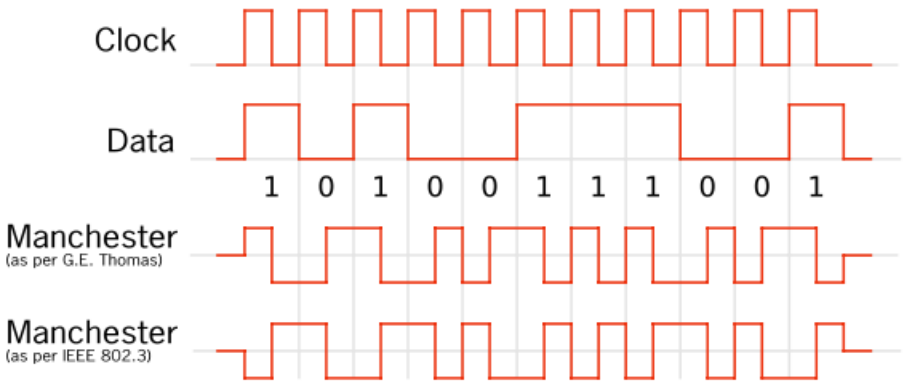
Tecnologías Ethernet

Estándar Ethernet	Fecha	Descripción
Ethernet experimental	1972 patentado en 1978	2,85 Mbit/s sobre cable coaxial en topología de bus.
Ethernet II (DIX v2.0)	1982	10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. Elprotocolo IP usa este formato de trama sobre cualquier medio.
IEEE 802.3	1983	10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.
802.3a	1985	10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 metros
802.3c	1985	Especificación de repetidores de 10 Mbit/s
802.3e	1987	1BASE5 o StarLAN
802.3i	1990	10BASE-T 10 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 150 metros.
802.3j	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
802.3x	1997	Full Duplex (Transmisión y recepción simultáneos) y control de flujo.
802.3y	1998	100BASE-T2 100 Mbit/s sobre par trenzado no blindado(UTP). Longitud máxima del segmento 100 metros
802.3z	1998	1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
802.3ab	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado
802.3ac	1998	Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estandar 802.1p.
802.3ae	2003	Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR
IEEE 802.3af	2003	Alimentación sobre Ethernet (PoE).
802.3ah	2004	Ethernet en la última milla.
802.3ak	2004	10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial.
802.3an	2006	10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado no blindado (UTP)

Sistema de codificación Manchester

- Codificación bifase-L para señales binarias en el que en cada período de bit hay una transición entre dos niveles de señal.
  - Se combinan señales de reloj y datos.
  - Cada bit posee una transición en la mitad de su período de reloj.
    - Una transición de negativo a positivo representa un dato 1 y una transición de positivo a negativo representa un dato 0

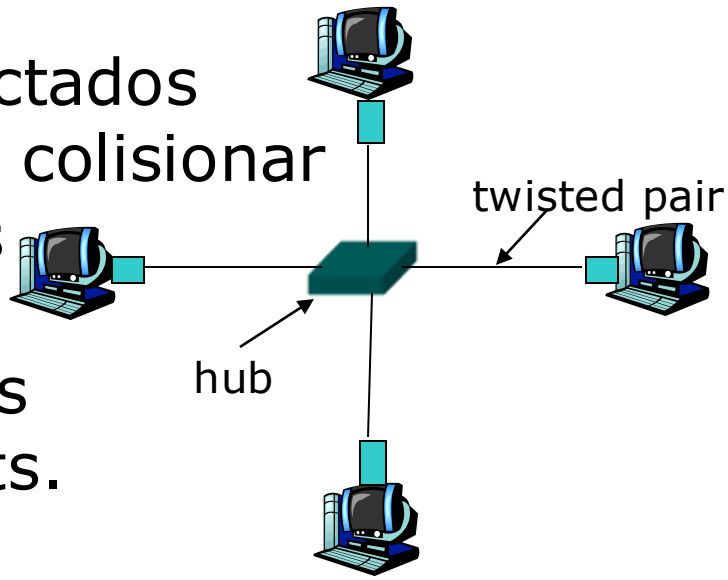
- Código Manchester = Datos XOR clk.
- Se utiliza en 10BaseT.
- Permite sincronizar relojes de emisor y receptor.
- Capa física



Índice

Conmutadores de capa física.

- Topologías modernas de redes LAN: estrella.
  - Cada nodo conectado a un conmutador central.
- El conmutador (hub) trabaja en capa física (repetidor):
  - Los bits que recibe por un enlace los reenvía al resto de enlaces a la misma velocidad.
  - Todos los nodos conectados al concentrador pueden colisionar
  - No dispone de buffers
  - El hub no aplica CSMA/CD. Lo aplican las tajetas NICs de los hosts.

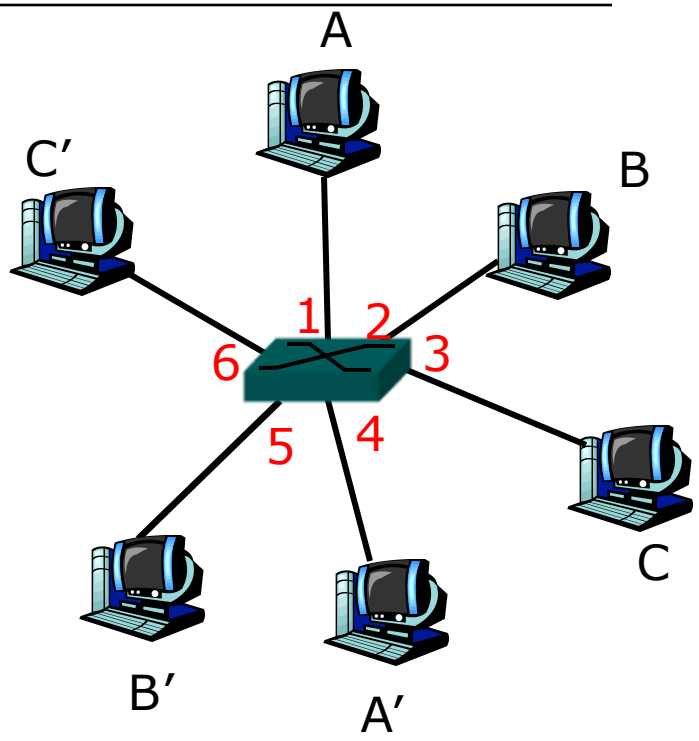


Conmutadores de capa de enlace.

- Un conmutador de capa de enlace de datos: switch. Más inteligente y activo que un hub.
  - Trabaja y almacena tramas Ethernet.
  - Analiza en las tramas que entran las MACs, y las redirige a uno o más enlaces.
  - Utiliza CSMA/CD.
  - Es transparente para los nodos (no son conscientes de la existencia de swich).
  - Capacidad de autoaprendizaje.
    - No necesitan ser configurados por un administrador

Conmutadores de capa de enlace.

- En topología estrella los hosts se conectan al switch.
- El switch almacena tramas en buffers.
- El protocolo Ethernet se utiliza en cada enlace aislado (full duplex). Nos hay colisión.
  - Cada enlace es un dominio de colisión.

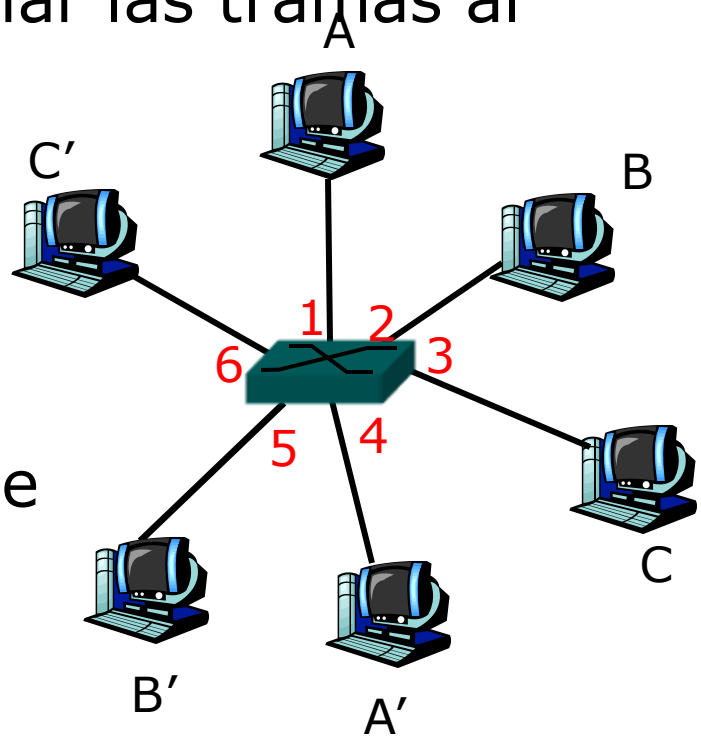


switch con 6 interfaces (1,2,3,4,5,6)

- Conmutación y transmisiones simultáneas sin colisiones.
  - Ejemplo: transmisiones B-B′ y C-C′

Conmutadores de capa de enlace.

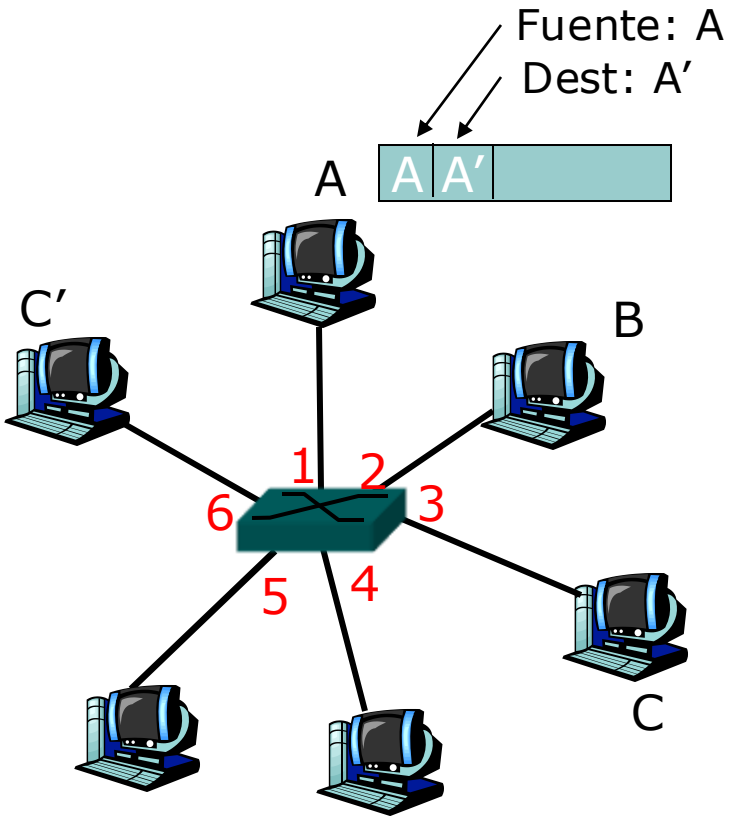
- Tabla de conmutación.
  - Permiten al switch enviar las tramas al host destino.
  - Cada entrada posee:
    - MAC destino.
    - Interface de salida.
    - Tiempo de registro en la tabla.
  - Semejante a la tabla de enrutamiento
  - Ejem: en transmisión A-A’ permite identificar el interface 4 se salida.
  - Las entradas en la tabla se crean automáticamente.



switch con 6 interfaces (1,2,3,4,5,6)

Conmutadores de capa de enlace.

- Autoaprendizaje:
  - Cada switch aprende los hosts que pueden alcanzarse por cada interface.
  - Inicialmente la tabla está vacía.
  - Cuando llega una trama de un host aprende automáticamente y la registra en la tabla.
  - El conmutador no tiene porqué tener registradas todos hosts en la tabla. El tiempo de envejecimiento provoca la eliminación de entradas



MAC addr	interface	TTL
A	1	60

Conmutadores. Funciones: filtrado y reenvío

- Filtrado: función del conmutador que determina si una trama debe ser reenviada a alguna interfaz o debe ser descartada.
- Reenvío: función del conmutador que determina las interfaces a las que una trama debe dirigirse y luego envía la trama a esas interfaces.
- Se utiliza la tabla del conmutador.

Conmutadores. Funciones: filtrado y reenvío

- Cuando una trama llega al conmutador por un interface:
  1. Registra en la tabla el enlace asociado con la MAC del emisor de la trama.
  2. A partir de la MAC de destino busca en la tabla del conmutador un registro.
  3. *if la MAC de destino se encuentra en la tabla.*

     then {

     if MAC destino coincide con la interface asociada en la tabla (la trama procede de un segmento de la LAN que contiene el host emisor)

     then ***filtrado***

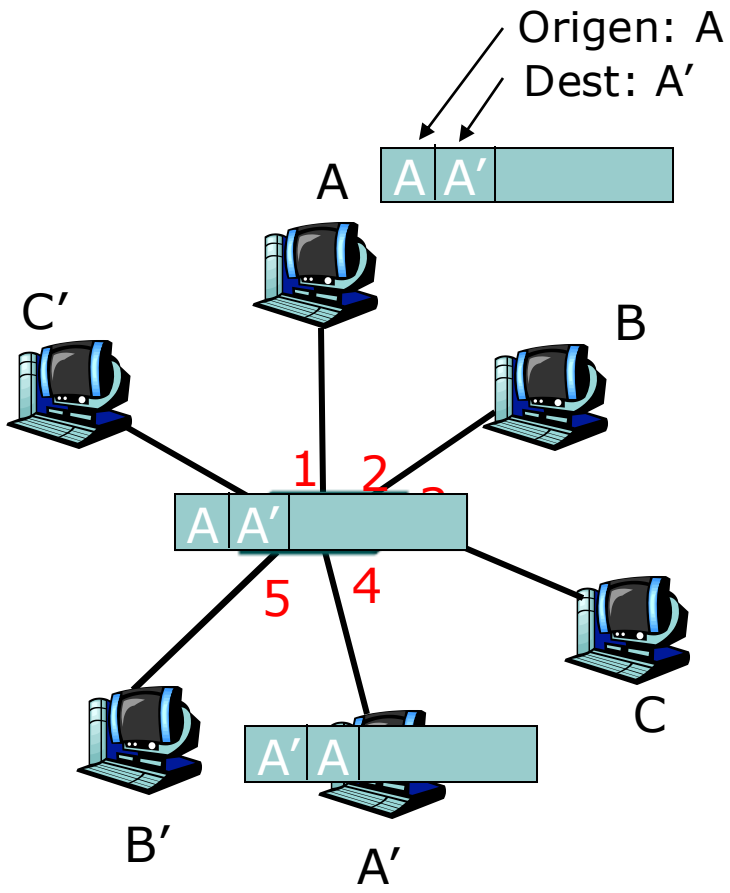
     else ***reenvío*** *a la interface adecuada*

     }

     else inundación (reenvío al resto de interfaces)

Conmutadores. Funciones: filtrado y reenvío

- Ejemplo:
  - MAC de destino desconocida : Inundación flooding.
  - MAC de destino conocida: Reenvío según Tabla MAC Mac-address-table.

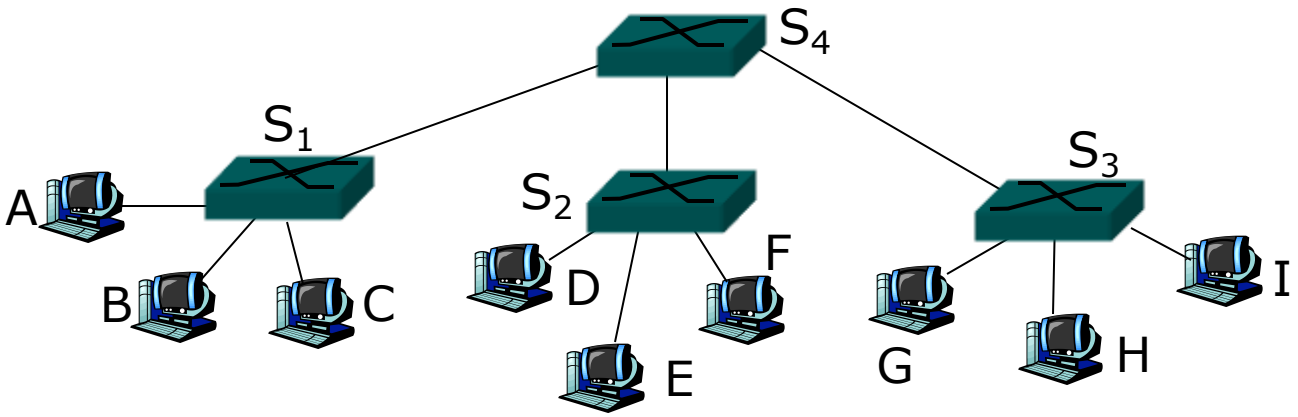


MAC addr	interface	TTL
A	1	60
A'	4	60

Tabla del conmutador (vacía al inicio)

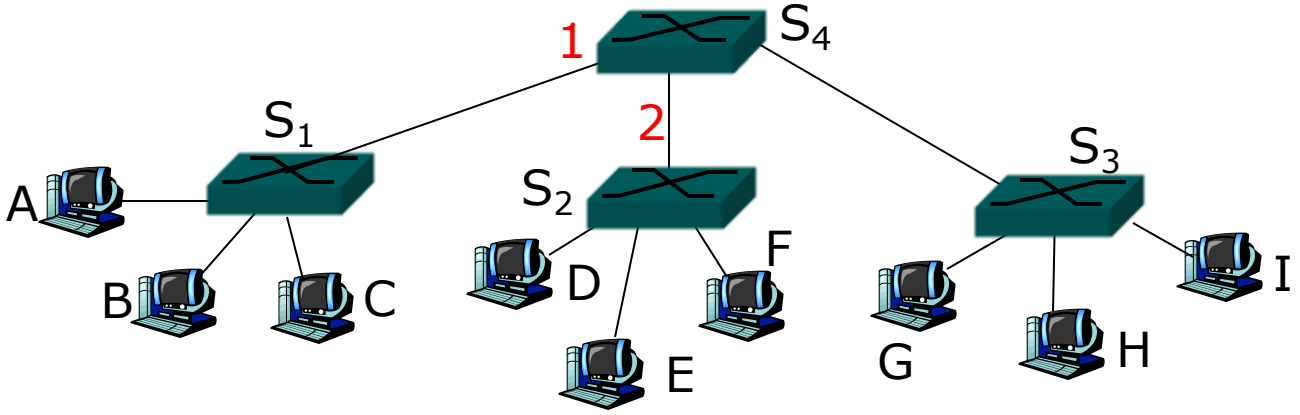
Conmutadores. Funciones: filtrado y reenvío.

- Ejemplo con interconexión de switches:
  - El host A envía una trama al host G pasando por los switches S4 y S3.

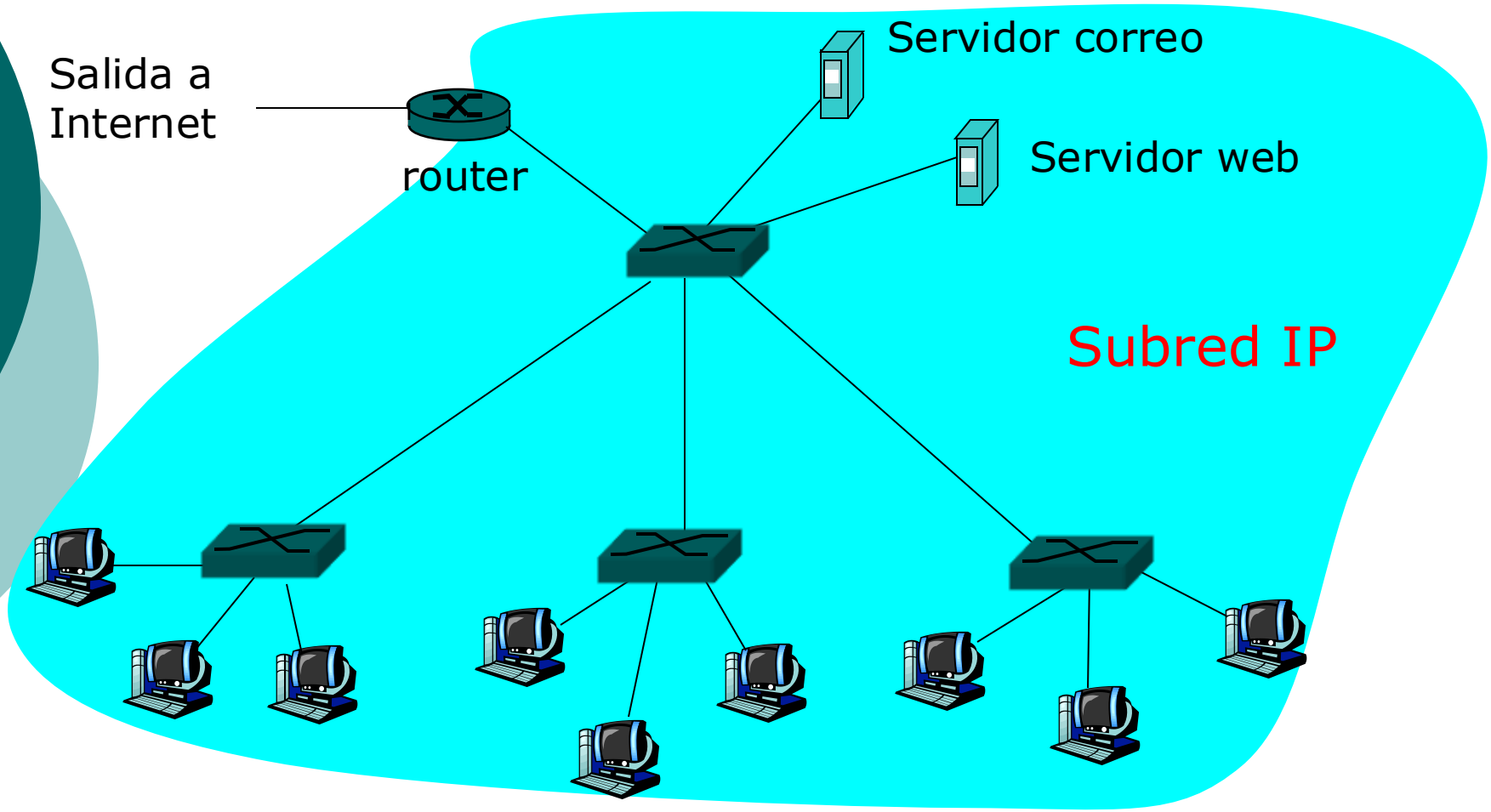


Conmutadores. Funciones: filtrado y reenvío.

- Ejemplo con interconexión de switches:
  - El host C envía una trama al host I.
  - Mostrar las tablas de conmutación en los switches S1, S2, S3, y S4.



Conmutadores en una red institucional.

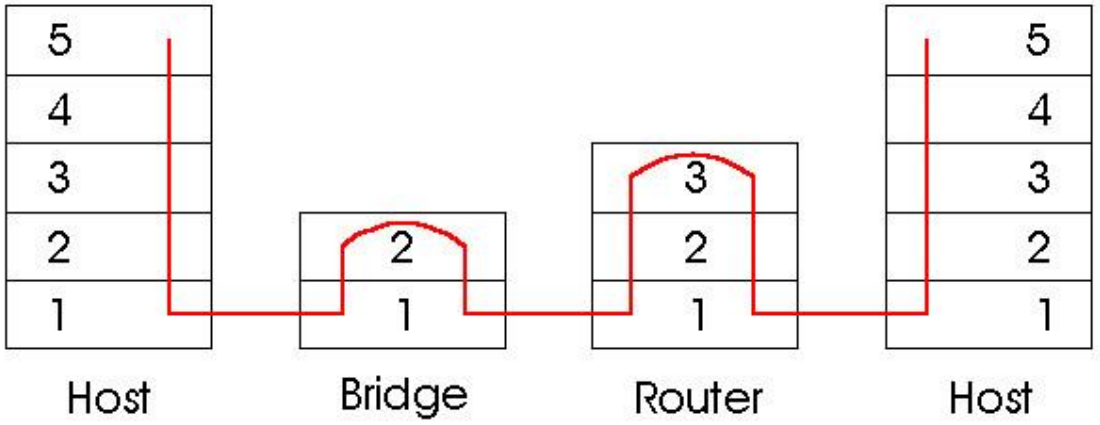


Ventajas de las redes con conmutadores

- Eliminación de colisiones: no se desperdicia ancho de banda
  - Se almacenan las tramas en los buffers.
  - No se transmite más de una trama a un segmento simultáneamente.
  - Tasa máxima de transferencia agregada del conmutador = suma de las tasas de los interfaces.
- Se permiten enlaces a distintas velocidades (10BASE-T, 1000 BASE-T) y medios físicos (100BASE-FX, 100BASE-T).
- Administración: permite administrar cada interface (desactivación, protección seguridad).

Conmutadores: routers y switches.

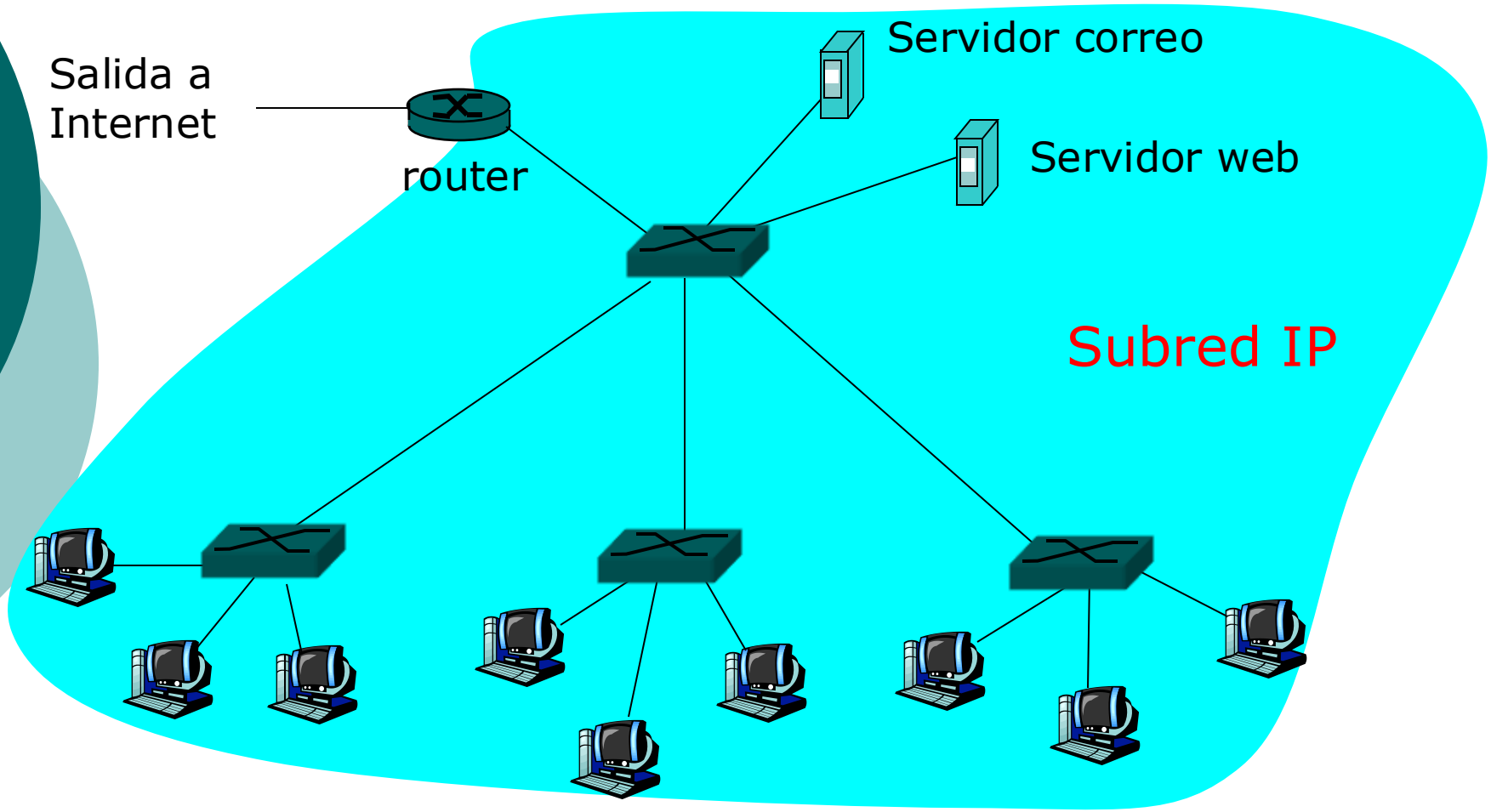
- Conmutadores: función de almacenamiento, filtrado y reenvío.
  - Router: dispositivos de capa de red (IPs de cabecera de datagrama).
  - Switches: dispositivos de capa enlace.
- Routers utilizan tablas de enrutamiento creadas con algoritmos de enrutamiento.
- Switches mantienen las tablas de conmutación, implementan filtrado y reenvío, algoritmos de auto-aprendizaje. Dispositivos plug-and-play.



Redes VLAN.

- VLAN: virtual local area network.
- Desventajas de una LAN conmutada.
  - Falta de aislamiento del tráfico. El tráfico de difusión (tramas ARP y DHCP y tramas sin aprender) tienen que atravesar toda la red.
    - Deseable limitar tráfico por seguridad y confidencialidad de grupos de trabajo (directivos y trabajadores).
  - Uso ineficiente de los conmutadores caso de estructurar la red en muchos grupos de trabajo con pocos hosts.
    - Ejemplo: crear muchos grupos de trabajo con 5 personas. Muchas interfaces del switch quedarían libres.
  - Gestión de usuarios: sin necesidad de recableado físico.
- VLAN soluciona estas desventajas: permite definir: múltiples redes de área local virtuales sobre una única infraestructura de red de área local física.

Red institucional.



Redes VLAN.

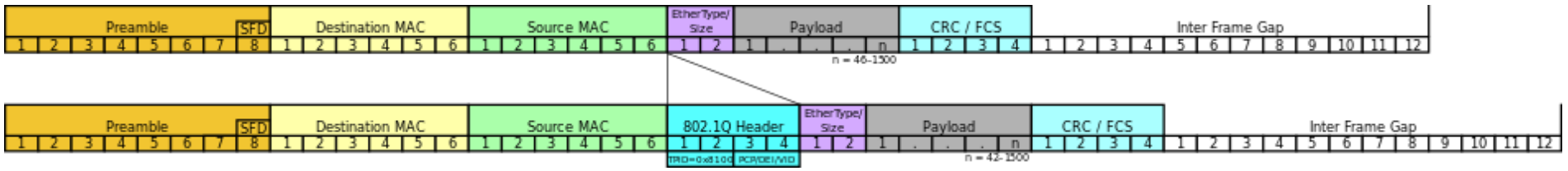
- Los hosts de una VLAN se comunican entre sí como si sólo ellos estuvieran conectados al switch.
  - El administrador divide los interfaces del conmutador en grupos VLANs (con ID y nombre).
  - Cada grupo en una VLAN formando un dominio de difusión: el tráfico broadcast de un interface sólo llega al resto de interfaces de la VLAN.
    - Ejemplo: un switch con 24 puertos.
      - Puertos 1-5 (modo acceso): VLAN -> Dpto. Mecánica.
      - Puertos 6-10 (modo acceso): VLAN -> Dpto. Derecho.
  - Los switches se interconectan mediante interfaces para transferir todo tipo de tráfico de las VLANs (puertos troncales).
  - Los puertos troncales pertenecen a todas las VLAN.
    - Todas las tramas enviadas a cualquier VLAN son reenviadas a través del enlace troncal hacia otros conmutadores.

Redes VLAN.

- Si se desea enviar tráfico entre hosts de una VLAN X a otra VLAN Y, se interconectan los switches a un router (enlaces troncales).
  - Solución alternativa: switch de capa 3.
- Etiquetado VLAN 802.1Q definido por IEEE.
  - Formada por la trama Ethernet más la **etiqueta VLAN**.
    - 4 bytes entre la **MAC de origen** y el campo **TIPO Ethertype**.
      - Campo TPID: Tag Protocol Identifier. 2 bytes.
        - IEEE 802.1Q: 0x8100.
      - Campo TCI: Tag Control Information.
        - 12 bits VID: VLAN ID. Identificador VLAN.
        - 3 bits PCP: Priority Code Pint. Prioridad (parecido a TOS en cabecera de datagrama). Valor 0: mejor esfuerzo (máxima prioridad. Valor 7: menor esfuerzo (mínima prioridad.
        - 1 bit DEI: Drop Eligible Indicatos. Bit para eleminar tramas (congestión).

Redes VLAN.

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID



Índice

Protocolo PPP

- Protocolos utilizado en enlaces punto a punto.
  - PPP: Point to Point Protocol.
  - HDLC: High-level Data Link Control.
- Más sencillos que los protocolos multipunto (canal compartido).
  - No requieren control al medio.
    - Son protocolos sin Media Access Control.
  - No necesitan direccionamiento explícito MAC.
  - Ejemplos: líneas ISDN, enlaces línea telefónica, enlace SONET/SDH, conexión X25, circuito RDSI.

Protocolo PPP. Requerimientos.

- Establecidos por IETF (RFC 1547):
  - Entramado de paquetes: el emisor debe encapsular paquete de nivel de red dentro de la trama de capa de enlace PPP. Receptor: desencapsulación.
  - Transparencia: PPP no debe aplicar restricciones a los datos de la PDU de nivel 2 (ni a cabecera, cola ni datos).
  - Múltiples protocolos de capa de red: multiplexado de varios protocolos. PPP debe ser compatible con IP, DECnet en el mismo enlace físico (equivale a decir que IP es compatible con TCP y UDP).
  - Múltiples tipos de enlaces: compatibilidad total sobre enlaces serie/paralelo, síncronos/asíncronos, cobre/fibra, baja/alta velocidad.

Protocolo PPP. Requerimientos.

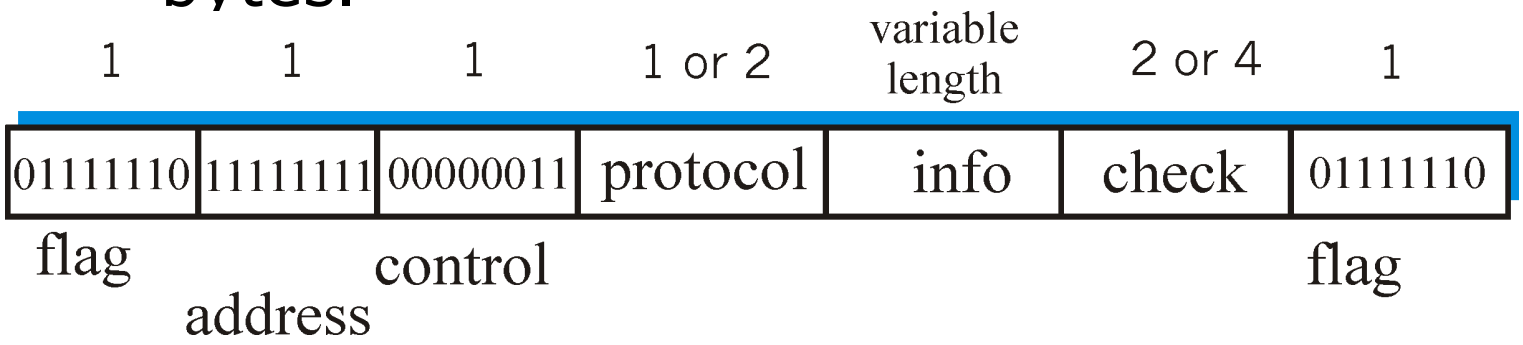
- Establecidos por IETF (RFC 1547):
  - Detección de errores: el receptor debe ser capaz de detectar errores de bit en las tramas recibidas.
  - Pervivencia de la conexión: PPP debe ser capaz de detectar fallo de conexión en el enlace e indicarlo a la capa de red.
  - Negociación de direcciones de la capa de red: debe proporcionar un mecanismo para que las capa de red (IP) que se están comunicando puedan aprender o configurar las direcciones de la capa de red de cada una de ellas.
  - Simplificidad.

Protocolo PPP. Requerimientos.

- Funcionalidades PPP sin implementar:
  - Corrección de errores.
  - Control de flujo: si una capa superior no puede recibir paquetes a la máxima velocidad proporcionada por capas inferiores, es su responsabilidad eliminar o controlar en el emisor el flujo de paquetes.
  - Secuenciamiento: no se requiere que PPP entre las tramas en el receptor en el mismo orden en que fueron enviadas por el emisor.
  - Enlaces multipunto: PPP sólo necesita un emisor y un receptor. HDLC puede operar con varios receptores.

Protocolo PPP. Trama.

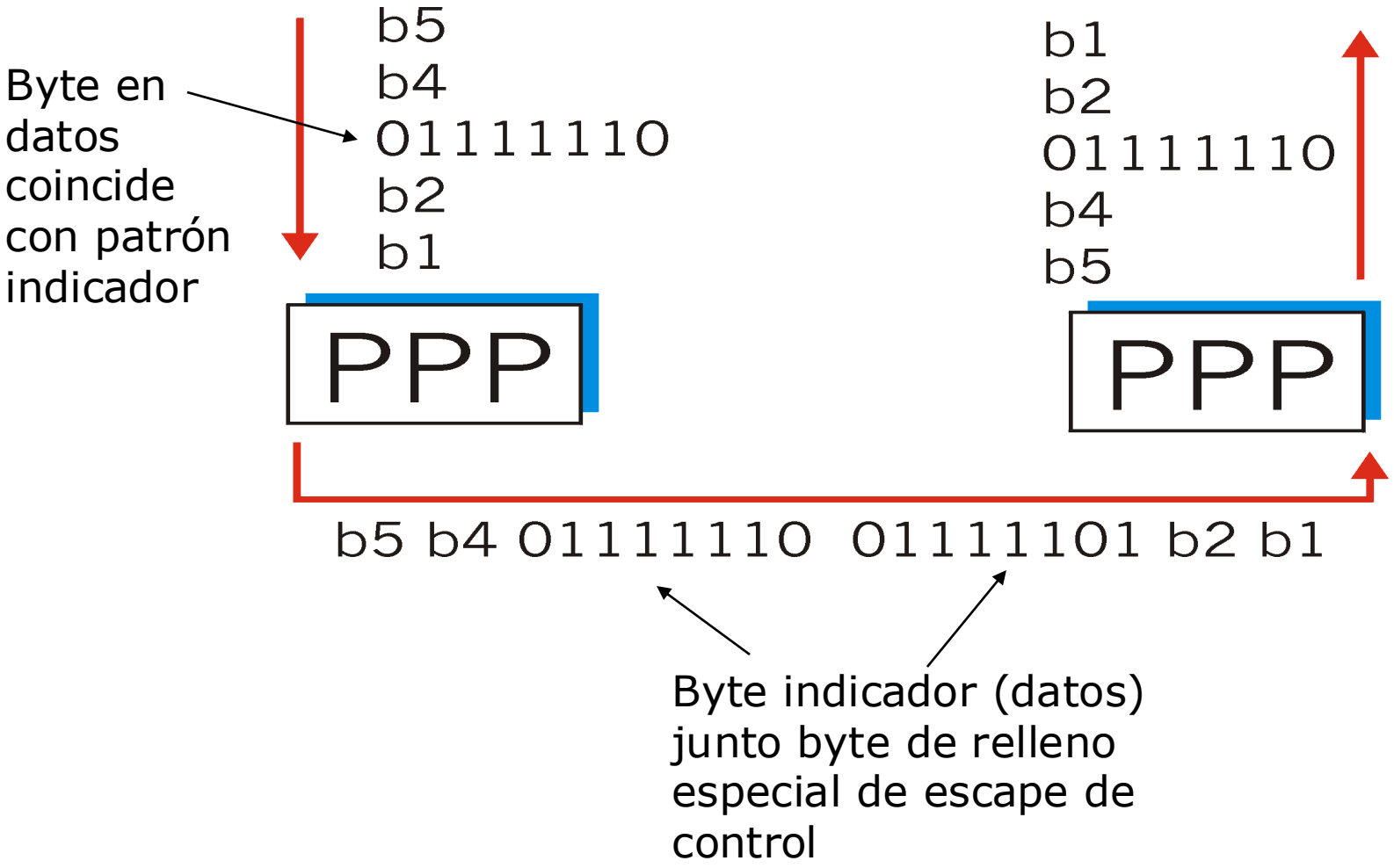
- Campos:
  - Indicador: de comienzo y fin = 01111110.
  - Dirección = 11111111.
  - Control = 00000011.
  - Protocolo: Protocolo de capa superior utilizado en los datos. IP=21, AppleTalk=29, DECnet=27.
  - Información: datos enviados por capa 3.
  - Suma de comprobación: CRC de 2 o 4 bytes.



Protocolo PPP. Rellenado de bytes.

- Problema: ¿Qué ocurre si un byte indicador de inicio y fin (patrón constante) aparece dentro de los datos (información)?
- Requisito transparencia no permite prohibir este patrón 01111110 en los datos información.
- Solución: técnica de rellenado de bytes.
  - Añadir un byte de escape de control 01111101 que precede al indicador.
    - Señala al receptor que el siguiente byte no es un indicador de comienzo o final. Es un byte de datos.
  - Si el byte de escape de control aparece en los datos reales, también se le antepone otro byte igual.

Protocolo PPP. Rellenado de bytes.



Bibliografía

- KUROSE, James F; ROSS, Keith W. Redes de computadoras. Un enfoque descendente. Pearson. Biba.
- Wikipedia contributors. Cyclic redundancy check [Internet]. Wikipedia, The Free Encyclopedia; 2015 Nov 3, 17:41 UTC [cited 2015 Nov 10]. Available from: https://en.wikipedia.org/w/index.php?title=Cyclic_redundancy_check&oldid=688890145.
- Wikipedia contributors. Channel access method [Internet]. Wikipedia, The Free Encyclopedia; 2015 Oct 30, 02:41 UTC [cited 2015 Nov 10]. Available from: https://en.wikipedia.org/w/index.php?title=Channel_access_method&oldid=688170319.