REDES DE COMPUTADORAS 1

Clase 6

Capa de Enlace

Objetivos

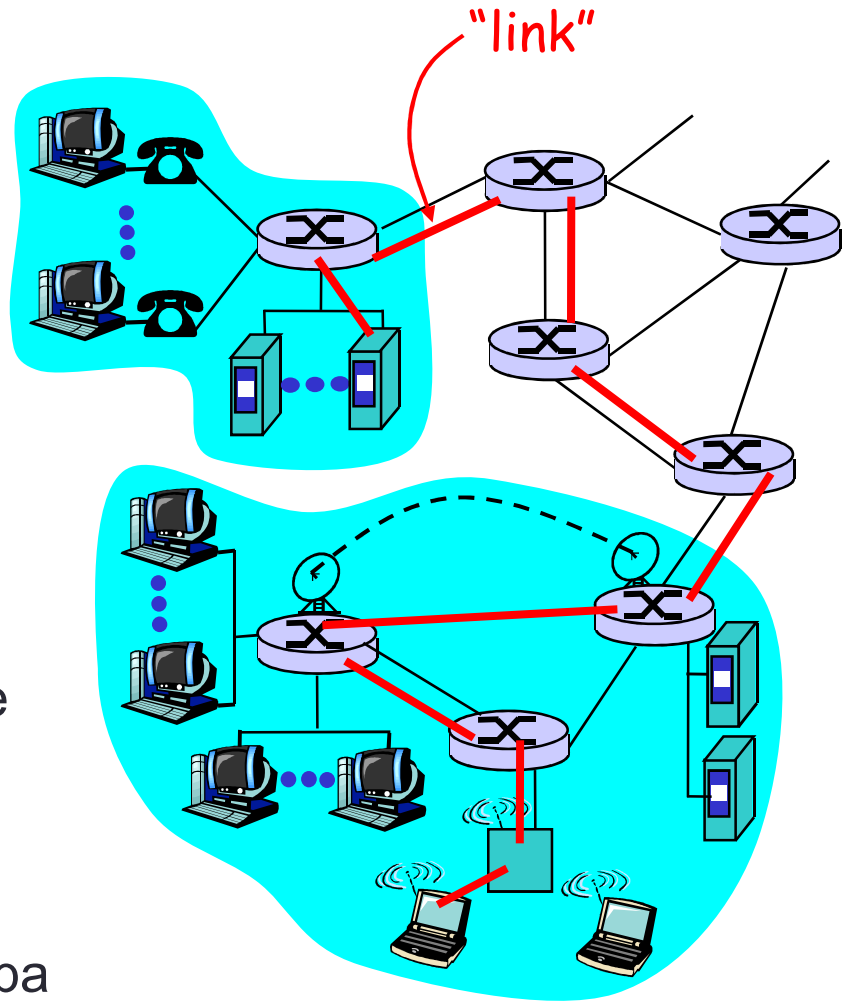
- Entender los principios detrás de los servicios de la capa enlace de datos:
  - Detección y corrección de errores
  - Compartición de canales broadcast: acceso múltiple
  - Direccionamiento de la capa enlace
  - Transferencia de datos confiable y control de flujo.
- Descripción e implementación de varias tecnologías de enlace

Agenda

- Introducción y servicios
- Detección y corrección de errores
- Protocolos de acceso múltiple
- Direccionamiento de capa enlace
- Ethernet
- Hubs y switches
- PPP
- Enlaces Virtuales

Capa de Enlace: Introducción

La capa de enlace de datos tiene la responsabilidad de transferir datagramas desde un nodo hacia el nodo adyacente a través de un enlace



Algo de terminología

- **Nodos:** hosts, routers y swiches.
- **Enlaces:** canales de comunicación que conectan nodos adyacentes a lo largo de un camino de comunicación.
  - Enlaces cableados
  - Enlaces inalámbricos
- **Trama (o frame):** es el paquete de la capa de enlace, que encapsula a los datagramas

Capa de Enlace: contexto

El protocolo de la capa de enlace define el formato de los paquetes intercambiados por los nodos extremos de un enlace, y las acciones que estos nodos llevan a cabo al enviar y recibir paquetes.

- Los datagramas son transferidos por diferentes protocolos de enlace en diferentes enlaces.
- Ejemplos de protocolos de capa de enlace son:
  - Ethernet
  - LAN inalámbricas 802.11 (WiFi)
  - Token ring
  - PPP.
- Cada protocolo de enlace provee servicios diferentes:
  - Ej: *puede o no proveer transferencia confiable sobre el enlace*

Capa de Enlace: servicios

- Entramado:
  - Encapsula un datagrama en una trama, agregando encabezados y cola.
- Acceso al enlace:
  - Protocolos de control de acceso al medio (MAC, *Medium Access Control*)
    - Enlaces punto a punto o de acceso múltiple.
    - Dirección “MAC” usada en encabezados de tramas para identificar fuente y destino.
      - ➔ Diferente a las direcciones IP

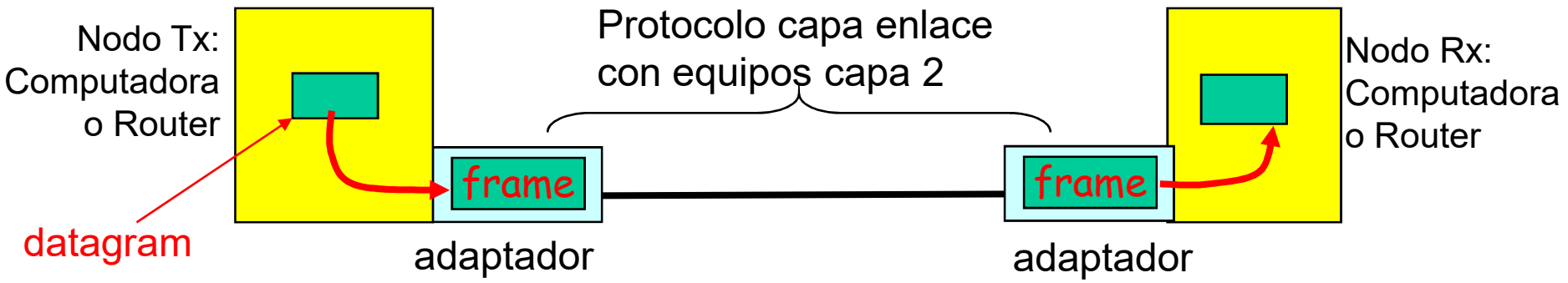
Capa de Enlace: servicios

- Entrega confiable:
  - Garantiza el transporte del datagrama a través del enlace sin errores (Entre nodos adyacentes).
  - Se utiliza en enlaces con altas tasas de error (ej: inalámbricos).
    - ➔ Pregunta: ¿por qué tener confiabilidad a nivel de enlace y extremo a extremo?
- Control de Flujo:
  - Capacidad limitada de almacenamiento en buffer de los nodos.
  - Proporciona un mecanismo de control de flujo para evitar que el nodo emisor abrume al nodo receptor (desborde del buffer del nodo receptor).

Capa de Enlace: servicios

- Detección de Errores:
  - Detección de errores de bit, causados por atenuación de señal y ruido.
    ➔ Pide al transmisor retransmisión o descartar la trama.
  - Es más sofisticada que la proporcionada por la capa de transporte y red.
  - Se implementa en hardware.
- Corrección de Errores (Forward error correction):
  - Receptor identifica y corrige error(es) de bit(s) sin solicitar retransmisión
    ➔ Requiere el envío de campos redundantes
- Semi-duplex y full-duplex:
  - Full-duplex ➔ los nodos de ambos extremos transmiten paquetes al mismo tiempo.
  - Semi-duplex ➔ los nodos no pueden transmitir y recibir al mismo tiempo.

Adaptadores de red

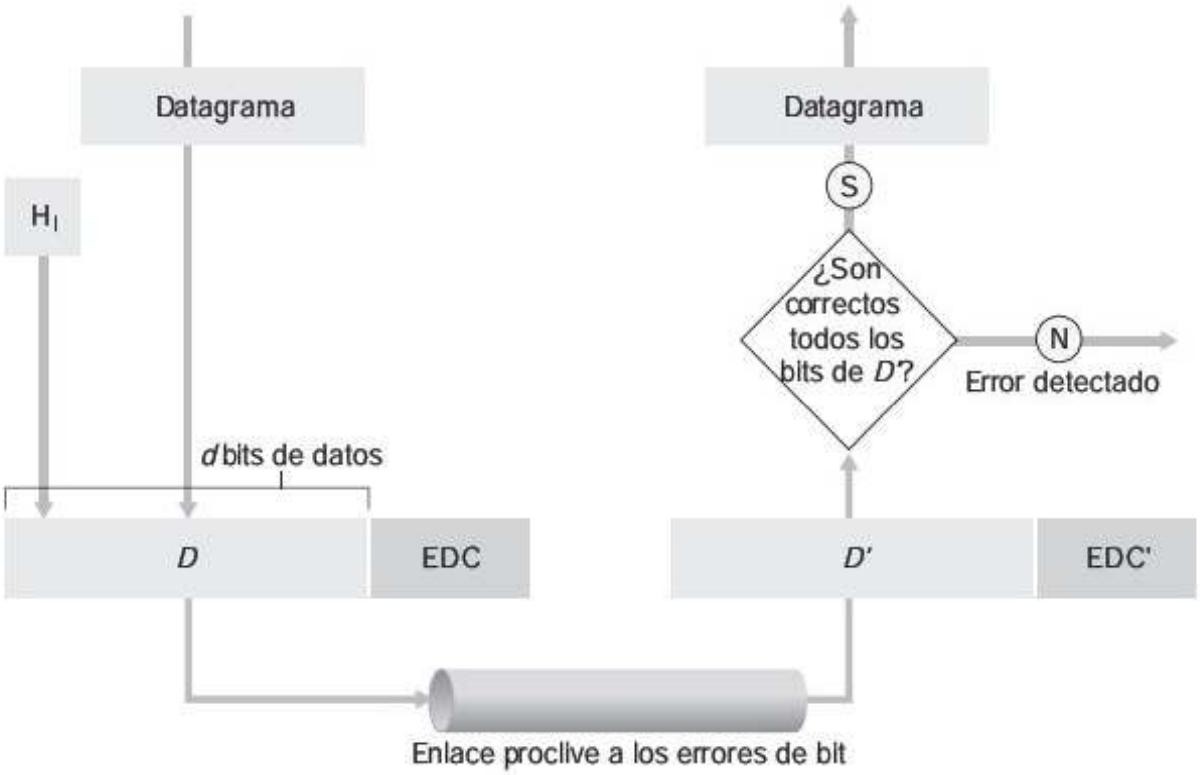


La capa de enlace es implementada mayoritariamente en un adaptador de red (NIC) ➔ Tarjetas Ethernet ó 802.11 (WiFi)

- Lado transmisor:
  - Encapsula el datagrama en una trama.
  - Agrega bits de chequeo de errores, control de flujo, etc.
  - Transmite la trama al enlace

- Lado receptor
  - Recibe la trama y extrae el datagrama.
  - Busca errores, control de flujo, etc
- El adaptador es semi-autónomo
- Capa enlace & capa física

Detección y corrección de errores



EDC: Error Detection and Correction bits (redundancia) - D: Datos a proteger.

Objetivo: determinar si *D'* coincide con *D*.

Detección y corrección de errores

- La detección de errores no es 100% confiable.
  - El protocolo puede ignorar algunos errores de bits.
  - Se busca elegir un esquema de detección de errores que minimice la probabilidad de error.
  - Técnicas más sofisticadas conducen a mejor detección y corrección de errores (campos EDC mayores y mayor cantidad de cálculos)

➔ *Estudiaremos 3 técnicas de detección de errores:*

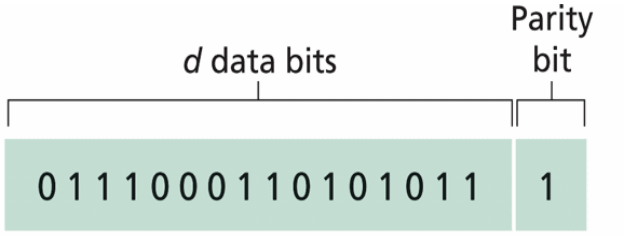
- ➔ Comprobación de paridad.
- ➔ Suma de comprobación (cheksum).
- ➔ Código de redundancia cíclica (CRC)

Comprobaciones de paridad

Bit de Paridad Simple:

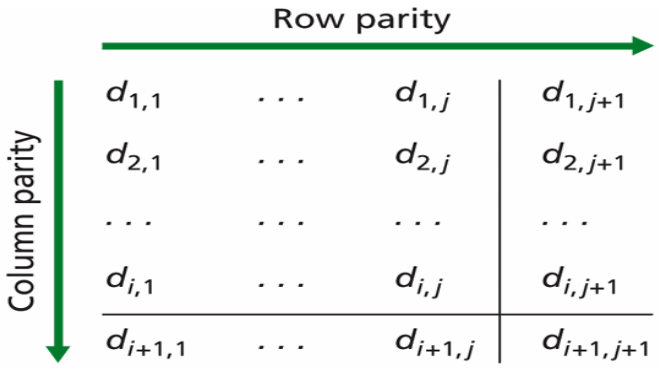
- **Detecta errores simples**
- **Se agrega 1 bit de paridad, tal que queden un número par (o impar) de bits en uno.**
- **Decimos que usamos paridad par o impar respectivamente.**

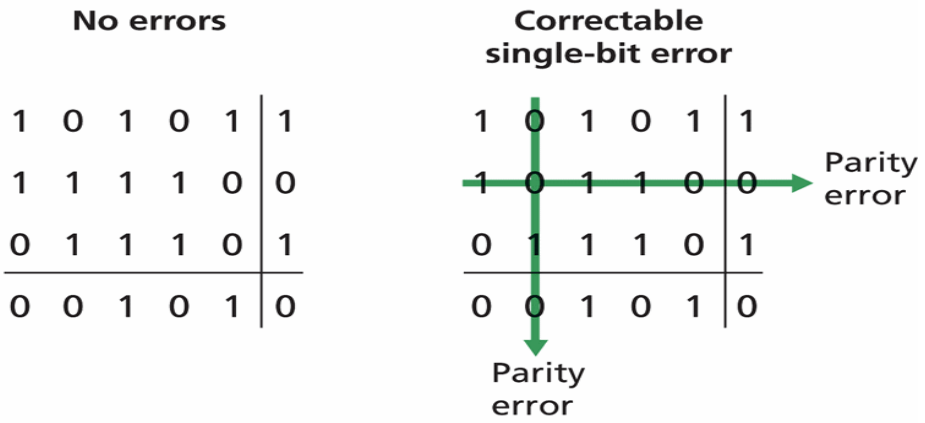
Los ejemplos mostrados dan paridad par.



Bit de paridad de dos dimensiones:

- **Detecta y corrige errores simples**





Sumas de comprobación: cheksum

Objetivo: detectar “errores” en segmentos transmitidos (típicamente usado en capa transporte – UDP y TCP)

Transmisor:

- Trata el contenido de los segmentos como una secuencia de enteros de 16 bits.
- Calcula el complemento a 1 de la suma de todas las palabras de 16 bits del segmento.
- Si se producen desbordamientos en las sumas se acarrean sobre el bit menos significativo.
- El resultado se almacena en el campo de checksum de UDP o UDP.
- En TCP y UDP las checksum se calcula sobre todos los campos (cabecera y datos).
- En IP la checksum se realiza sobre la cabecera IP solamente.

Sumas de comprobación: cheksum

Receptor:

- Calcula la suma de todas las palabras de 16 bits recibidas, incluida la checksum.
- Si no se han introducido errores en el paquete, entonces la suma del receptor tiene que dar todos 1's.
- Si hay algún 0 ➔ error detectado
- SI hay todos 1 's ➔ no se detectó error (¿ ….Pero podría haberlo?)

- ➢ Requiere relativamente poca sobrecarga.
- ➢ Protección relativamente débil.

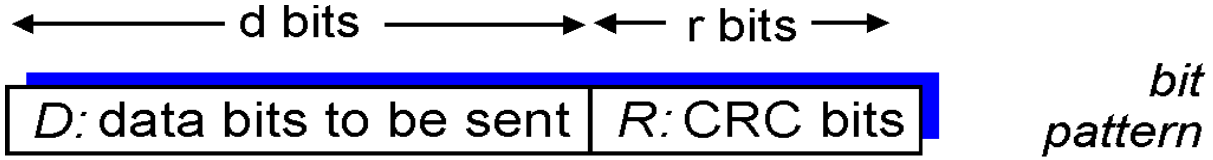
Comprobación de redundancia cíclica (CRC)

Trata a los bits de datos (D) como *polinomios* con coeficientes 0 o 1.

➔ Utiliza aritmética de polinomios en las operaciones realizadas

PROCEDIMIENTO:

- Se elige un patrón (generador) de (r+1) bits, G
  - el MSB (bit mas significativo) de G debe ser 1
- Se eligen r bits adicionales (R) que se agregan a los datos, tal que:
  - <D,R> sea exactamente divisible por G (en aritmética módulo 2)
  - Receptor: divide <D,R> por G. Si resto es no cero: hay error detectado!
  - Puede detectar secuencias de errores menores que r+1 bits
- Ampliamente usado en la práctica en capa enlace (ej. ATM, HDCL)



bit pattern

$D * 2^r$ XOR R

mathematical formula

CRC: ¿Cómo encontrar G?

Todas las sumas y restas se hacen bit a bit sin acarreo (aritmét. Módulo 2)

$$(A + B = A - B = A \text{ XOR } B)$$

- *Queremos encontrar R tal que:*

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

- *Equivalentemente:*

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

- *Es decir: R es el resto de la división:* ***D.2^r dividido G***

$$R = \text{resto}\left[\frac{D \cdot 2^r}{G}\right]$$

CRC: ¿Cómo encontrar G?

Transmisor:

- Dados los bits de datos D.
- Definido el patrón generador G.
- Se calcula el resto de la división ***D.2^r dividido G.***
- *Se* arma el EDC como <D,R>.

Receptor

- Se divide <D,R> por G.
- Si el resto de esta división es distinta de cero ➔ hubo un error.
- Si el resto de esta división es igual a cero ➔ no se detecta error.

CRC: ejemplo

D = 101110 G = 1001 r = 3 bits

```
101110000:1001=101011
1001
 101
 000
 1010
 1001
  110
  000
  1100
  1001
   1010
   1001
    011
```

D

G

R

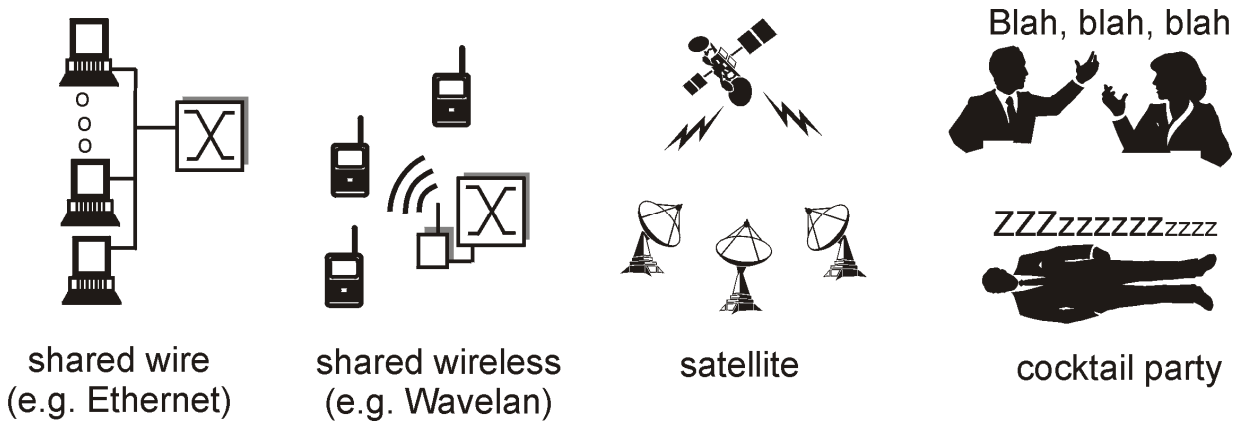
Verificación (Receptor):

```
101110011:1001=101011
1001
 0101
 0000
  1010
  1001
   0110
   0000
    1101
    1001
     1001
     1001
      000 => Resto
```

Protocolos de Acceso Múltiple

Dos tipos de “enlaces” físicos :

- Punto-a-apunto
  - Acceso discado usando Point-to-Point Protocol (PPP)
  - Enlaces punto-a-punto entre switch Ethernet y host (computadora)
- Broadcast (cable o medio compartido)
  - Múltiples nodos emisores y receptores conectados a un único enlace.
  - Ethernet y redes LAN inalámbricas son ejemplos de acceso múltiple.
  - Flujo de subida en HFC (***H**ybrid **F**iber **C**oax)*



Protocolos de Acceso Múltiple

- Usan un canal simple de difusión compartido
- Puede haber dos o más transmisiones simultáneas en distintos nodos ➔ Interferencia
  - colisión si un nodo recibe dos o más señales al mismo tiempo

Protocolos de acceso múltiple

- Algoritmo distribuido que determina cómo los nodos comparten el canal, es decir determina cuándo un nodo puede transmitir
- Son los mensajes para ponerse de acuerdo sobre cómo compartir el mismo canal!
  - no hay un canal “fuera de banda” para coordinación

Protocolo de Acceso Múltiple Ideal

Supongamos un canal broadcast de tasa R bps, el caso IDEAL es:

1. Cuando un nodo quiere transmitir, éste puede enviar a tasa R.
2. Cuando M nodos quieren transmitir, cada uno puede enviar en promedio a una tasa R/M
3. Completamente descentralizado:
   - No hay nodo especial para coordinar transmisiones
   - No hay sincronización de reloj o ranuras
4. Protocolo simple, de modo que no sea costoso implementarlo.

➔ Este ideal no existe, pero define el máximo teórico.

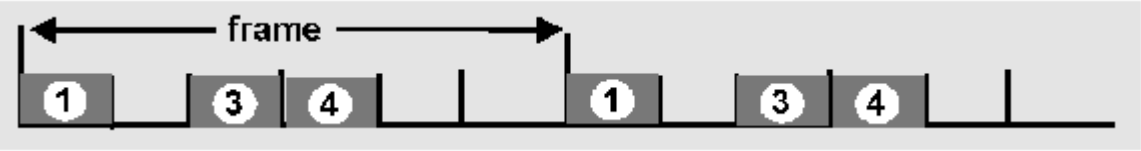
Taxonomía de protocolos MAC (Media Access Control)

Tres clases amplias:

- Canal Subdividido (“particionado”)
  - Divide el canal en pequeños “pedazos” (TDMA/FDMA/CDMA)
  - Asigna pedazos a un nodo para su uso exclusivo.
  - Cada nodo transmitirá a R/N (Siempre - aunque sea el único que transmite).
- Acceso Aleatorio
  - Canal no es dividido, permite colisiones.
  - Todos transmiten a máxima velocidad del canal (R)
  - Hay que “recuperarse” de las colisiones
- “Tomando turnos”
  - Los nodos toman turnos, pero nodos con más por enviar pueden tomar turnos más largos

Protocolos de particionamiento del canal: TDMA

- Acceso a canales es en “rondas“.
- Cada nodo obtiene una ranura de largo fijo (largo= tiempo transmisión del paquete) en cada ronda.
  - Se evitan las colisiones.
  - Se distribuye equitativamente los recursos.
  - Ranuras no usadas no se aprovechan.
  - Se limita la tasa de transferencia a R/N para todos los nodos.
  - Cada nodo siempre tiene que esperar su turno para transmitir.

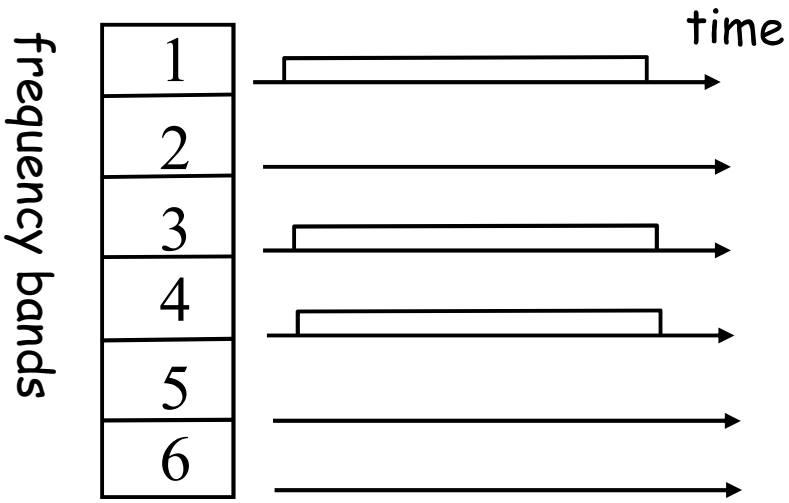


Ej. Reserva de esta aula para clases

Protocolos de particionamiento del canal: FDMA

- Espectro del canal es dividido en bandas de frecuencia.
- Cada estación obtiene una banda de frecuencia fija.
  - La banda de frecuencia de transmisión no usada no es aprovechada.
  - Ventajas y desventajas: similares a TDMA.

Ej.: Canales de televisión



Protocolos de Accesos Aleatorio (MAC)

- Cuando un nodo tiene paquetes que enviar
  - Transmite a la tasa máxima del canal, R.
  - No hay coordinación entre nodos
- Si dos o más nodos transmiten se produce “colisión”.
  - Cada nodo retransmite su trama hasta que consiga pasar.
- Protocolos de acceso aleatorio especifican:
  - Cómo detectar colisiones
  - Cómo recuperarse de una colisión (ej., vía retransmisiones retardadas)
- Ejemplos de protocolos MAC de acceso aleatorio:
  - ALOHA ranurado
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA (CSMA: Carrier Sense Multiple Access – Acceso múltiple con sondeo de portadora)

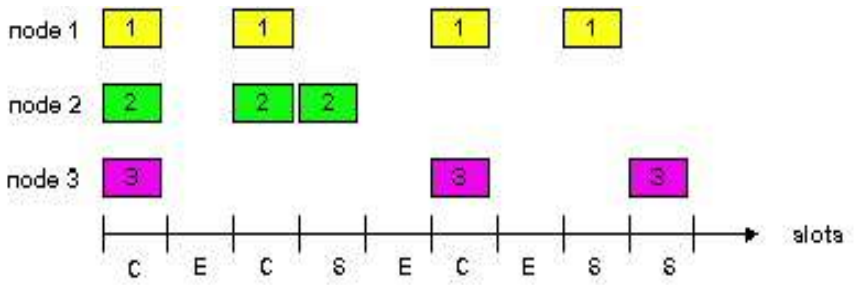
ALOHA ranurado

Suposiciones

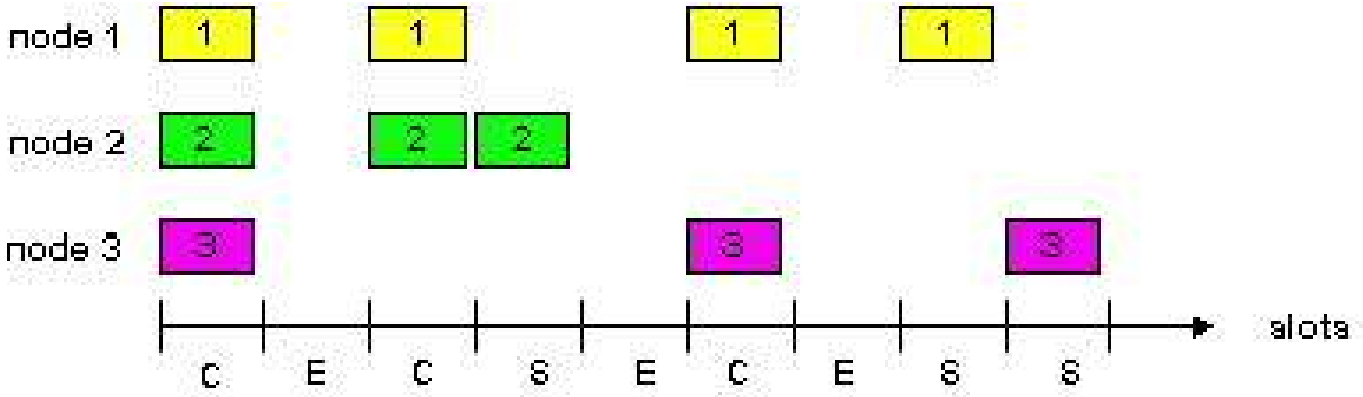
- Todos las tramas tienen igual tamaño.
- Tiempo es dividido en ranuras de igual tamaño = tiempo que se tarde en enviar una trama.
- Nodos comienzan a transmitir sólo al inicio de cada ranura.
- **Nodos están sincronizados**
- Si 2 ó más nodos transmiten en una ranura, todos los nodos detectan la colisión

Operación

- Cuando un nodo obtiene una trama nueva a enviar, éste transmite en próxima ranura.
- Si no hay colisión, el nodo puede enviar una nueva trama en próxima ranura.
- Si hay colisión, el nodo retransmite la trama en cada ranura siguiente con probabilidad p hasta transmisión exitosa.



ALOHA ranurado



Ventajas

- Un único nodo activo puede transmitir continuamente a tasa máxima del canal.
- Altamente descentralizado.
- Simple.

Desventajas

- Colisiones, las ranuras se desperdician.
- Ranuras no ocupadas.
- Nodos podrían detectar la colisión en menor tiempo que el de transmitir un paquete.
- Requiere la sincronización de todos los nodos.

Eficiencia de ALOHA ranurado

Eficiencia fracción (a largo plazo) de uso exitoso de ranuras cuando hay muchos nodos y cada uno tiene muchas tramas para enviar

- Supongamos N nodos con muchas tramas a enviar, cada una transmite con probabilidad *p*
- Simplificación para el cálculo
- Probabilidad de que SOLO el nodo 1 tenga éxito en un slot es $p(1-p)^{N-1}$
- Probabilidad de que exactamente uno de los N nodos tenga éxito es $Np(1-p)^{N-1}$

- Con N nodos activos la Eficiencia es: $E(p)= Np(1-p)^{N-1}$
- Para encontrar la máxima Eficiencia se debe encontrar p* que maximiza E(p).
- Para muchos nodos, tomar límite de $Np^*(1-p^*)^{N-1}$ cuando $N \rightarrow \infty$

Máxima eficiencia = 1/e = 0,37

Mejor caso: transmisiones útiles el 37% del tiempo!

➔ La velocidad efectiva óptima del canal es 0,37R

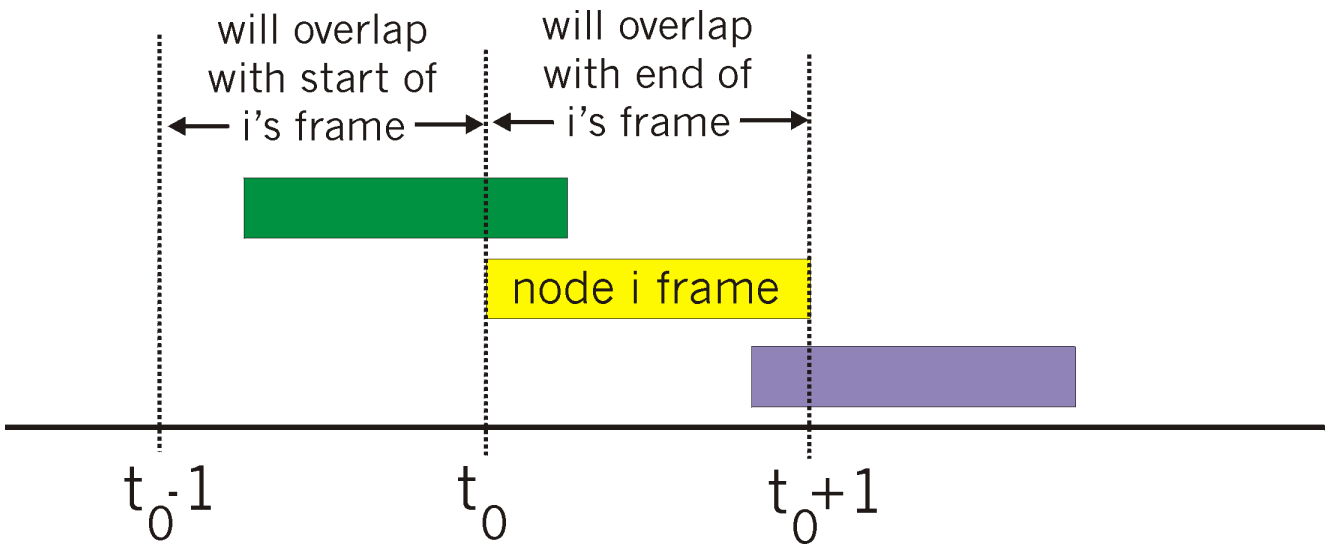
ALOHA Puro (no ranurado)

- Aloha no ranurado: más simple, no hay sincronización.
- Cada trama que debe ser enviada

  ➔ Se transmite inmediatamente
- Si la trama colisiona
  - ➔ Se espera a que termine la transmisión que colisionó
  - ➔ Se transmite la trama con probabilidad p
  - ➔ o no se transmite con probabilidad 1-p
- Si la trama no se retransmitió:
  - ➔ Se espera un tiempo igual al tiempo de trama
  - ➔ Se transmite la trama con probabilidad p
  - ➔ o se espera otro período igual con probabilidad 1-p

ALOHA Puro (no ranurado)

- La probabilidad de colisión aumenta:
  - La trama enviada en t_0 colisionara con.
    - ➔ Otras tramas enviadas antes de t_0
    - ➔ Otras tramas enviadas después de t_0



Eficiencia de ALOHA puro

P(e): Probabilidad de éxito en la transmisión:

$$P(e) = p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1} = p \cdot (1-p)^{2(N-1)}$$

- p: P(transmita nodo i)
- $(1-p)^{N-1}$: P(nadie transmita en $[t_0-1 , t_0]$)
- $(1-p)^{N-1}$: P(nadie transmita en $[t_0 , t_0+1]$)

- Encontrando el valor de p óptimo y tomando el límite para cuando se tienen muchos nodos:

$$E(p^*) = 1/(2e) = 0,18$$

¡La mitad que para ALOHA ranurado!

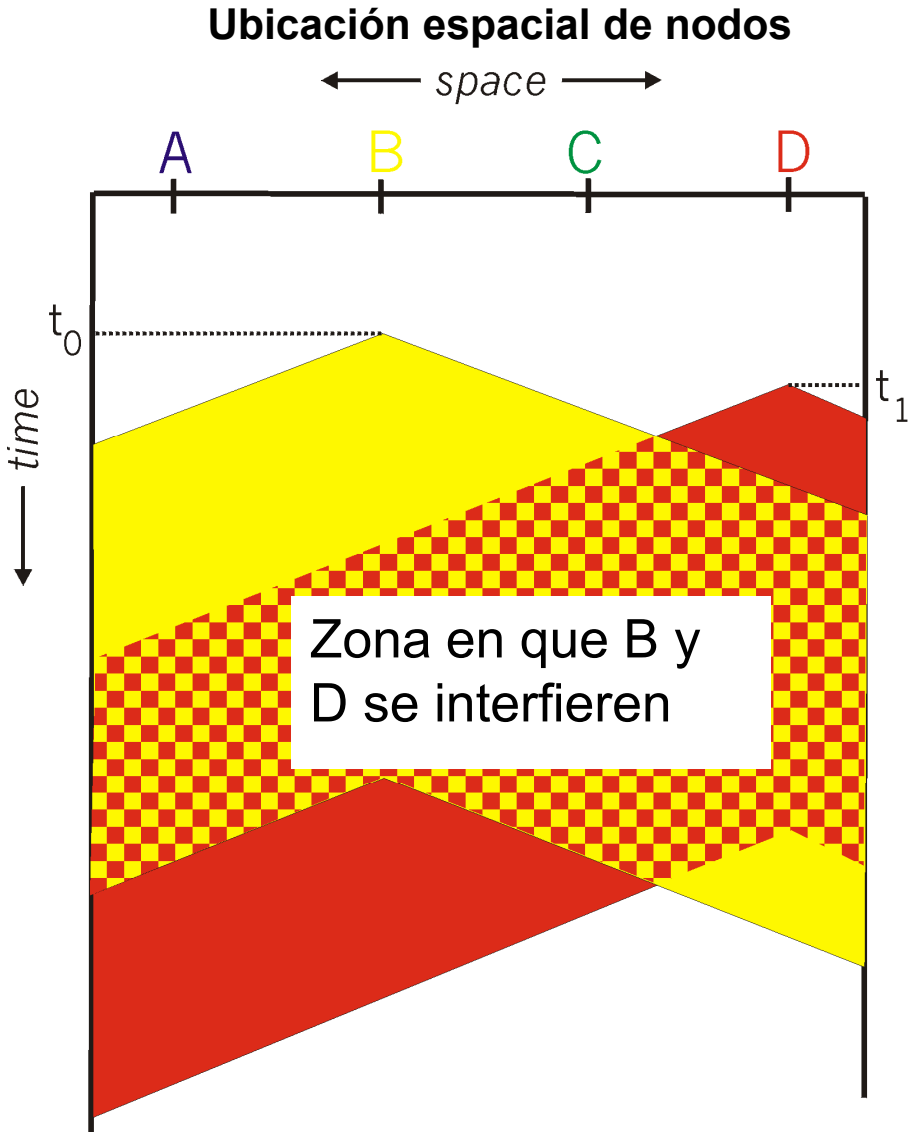
Acceso múltiple con acarreo de portadora (CSMA)

Se basan en dos reglas básicas:

- Sondeo de portadora:
  - Cada nodo sondea el canal antes de transmitir.
  - Si el canal se detecta libre ➔ se transmite la **trama entera**.
  - Si el canal se detecta ocupado ➔ se posterga transmisión (un tiempo aleatorio).
- Analogía humana ➔ no interrumpir mientras otros hablan!

Colisiones en CSMA

- Igual Colisiones pueden ocurrir:
  El retardo de propagación hace que dos nodos podrían no escuchar sus transmisiones
- En caso de Colisión:
  El tiempo de transmisión del paquete entero es desaprovechado
- Notar el rol de la distancia y el retardo de propagación en la determinación de la probabilidad de colisión

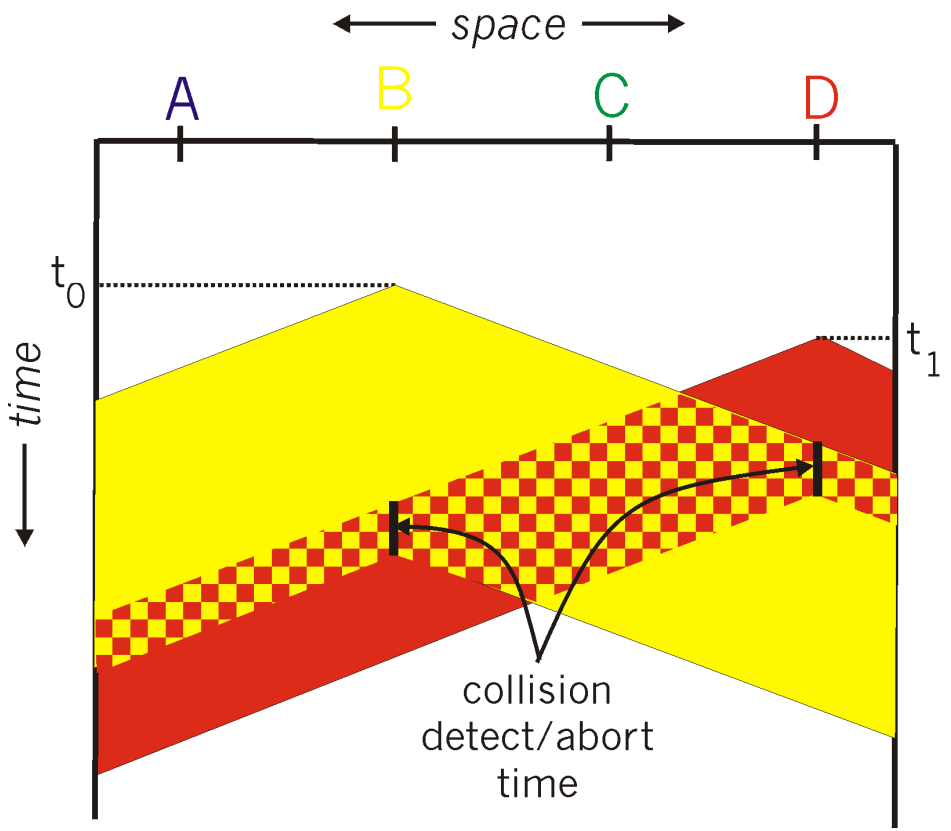


CSMA/CD (Detección de colisiones)

Similar a CSMA más detección de colisiones

- Detección de colisiones:
  - Un nodo que está transmitiendo ➔ sigue sondeando el canal mientras transmite.
  - Si detecta que otro nodo también transmite ➔ detiene la transmisión.
- Consecuencias:
  - Las colisiones son detectadas en menor tiempo.
  - Se reduce el mal uso del canal (comparado con sólo CSMA).
- En la práctica:
  - Fácil en LANs cableadas: se mide la potencia de la señal, se compara señales transmitidas con recibidas
  - Difícil LANs inalámbricas: receptor es apagado mientras se transmite

CSMA/CD (Detección de colisiones)



Protocolos MAC de “toma de turnos”

Vimos: Protocolos MAC que particionan el canal:

- Se comparte el canal eficientemente y equitativamente en alta carga
- Son ineficiente a baja carga: Hay retardo en acceso al canal, la tasa de transferencia asignada es R/N aún si hay sólo un nodo activo!

Vimos: Protocolos de acceso aleatorio

- Son eficientes a baja carga: un único canal puede utilizar completamente el canal
- Alta carga: ineficiencias por colisiones

Idea: Protocolos de “toma de turnos”

- Buscan lo mejor de ambos mundos!

Protocolos MAC de “toma de turnos”

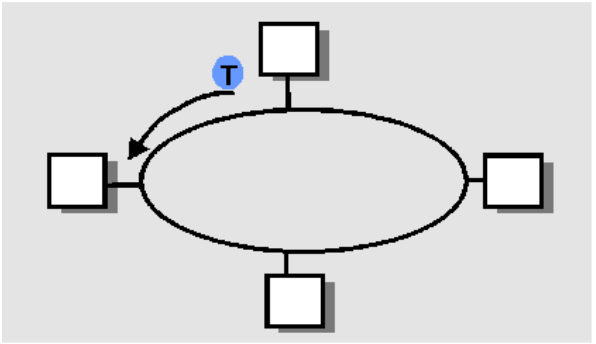
Protocolo de Sondeo:

- Nodo maestro
  - “invita” a nodos esclavos a transmitir en turnos.
  - Limita la cantidad de tramas que pueden transmitir dichos nodos.
  - Detecta si un nodo dejo de transmitir.
- Ventajas:
  - Elimina colisiones y particiones vacías.
  - Mejora eficiencia.
- Desventajas:
  - Retardo de sondeo.
  - Latencia.
  - Punto único de falla (maestro).

Protocolos MAC de “toma de turnos”

Paso de Testigo (Token):

- Testigo (Token):
  - Trama de pequeño tamaño.
  - Es pasado de nodo en nodo secuencialmente.
  - Cada nodo transmite sus tramas mientras tiene en posesión el testigo.
  - Existe un límite máximo de tramas que puede transmitir cada nodo.
- Ventajas:
  - Descentralizado
  - Altamente eficiente.
- Desventajas:
  - La falla de un nodo puede hacer que falle todo el canal.
  - Olvido del token.



Resumen de protocolos MAC

- ¿Qué hacemos en un medio compartido?
  - Subdivisión del canal: por tiempo, frecuencia, o código
  - Subdivisión aleatoria (dinámica),
    - ALOHA, ALOHA-R, CSMA, CSMA/CD
    - Sensado de portadora: fácil en algunas tecnologías (cable), difícil en otras (inalámbricas)
    - CSMA/CD (collision detection) es usado en Ethernet
    - CSMA/CA (collision avoidance) es usado en 802.11
  - Toma de turnos
    - Consultas desde un sitio central, o pasando un token