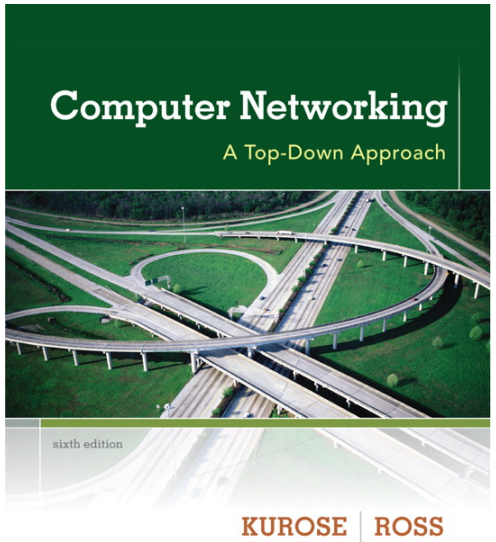
Capítulo 5: Capa de enlace



A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a lot of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

Capítulo 5: capa de enlace

objetivos:

- Entender los servicios que brinda la capa de enlace:
  - detección de errores, corrección
  - compartiendo un canal de difusión: acceso múltiple
  - direccionamiento en la capa de enlace
  - red de área local: ethernet, VLANs
- Protocolos de acceso al medio

Capa de enlace: ruta

5.1 introducción, servicios

5.2 detección de errores, corrección

5.3 protocolos de acceso múltiple

5.4 LANs

- direccionamiento, ARP
- ethernet
- switches
- VLANS

5.5 enlace de virtualización: MPLS

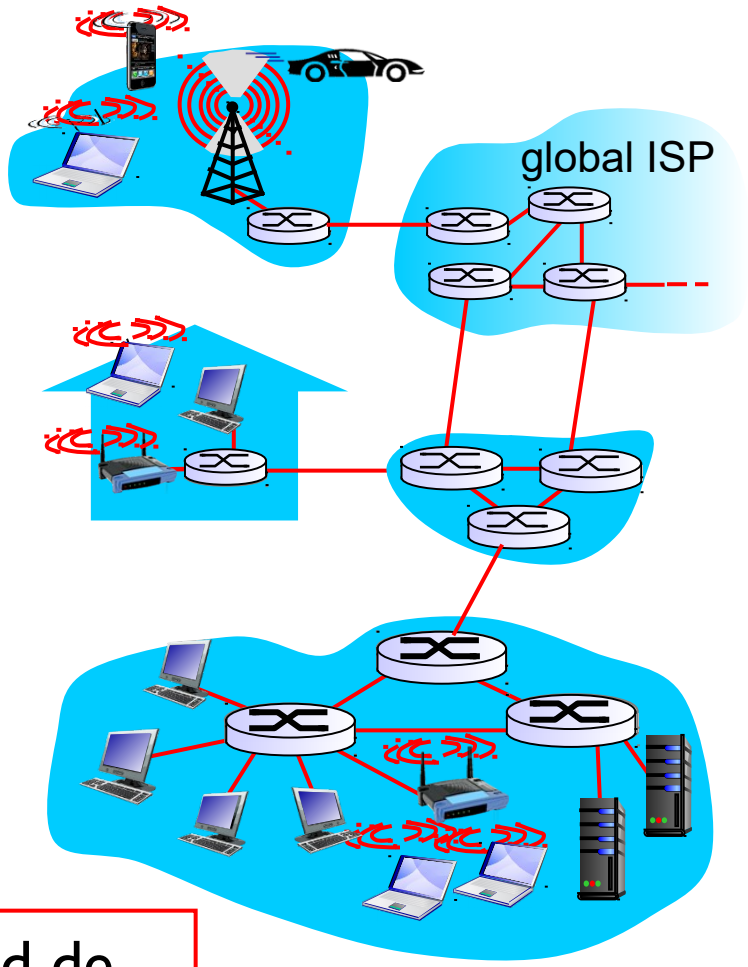
5.6 redes de centros de datos

5.7 un día en la vida de una solicitud web

Capa de enlace: introducción

terminología:

- equipos y enrutadores: nodos
- canales de comunicación que comunican enlaces adyacentes: enlaces
  - Enlaces cableados
  - Enlaces inalámbricos
  - LANs
- paquetes de capa 2: trama (frame), datagramas encapsulados
- El protocolo de la capa de enlace define el formato de los paquetes intercambiados por los nodos situados en los extremos del enlace, así como las acciones que estos nodos llevan a cabo cuando se envían y reciben los paquetes.



capa enlace-datos tiene la responsabilidad de transferir datagramas de un nodo a otro nodo *físicamente adyacentes* sobre un enlace

Capa de enlace: contexto

- Los datagramas son transferidos por diferentes medios de enlace y se utilizan diferentes protocolos dependiendo del enlace utilizado:
  - e.g., Ethernet en el primer enlace, frame relay en los enlaces intermedios y 802.11 en último enlace
- cada protocolo de enlace provee diferentes servicios

Analogía de transporte:

- un viaje de Princeton a Lausanne
  - limocina: Princeton al JFK
  - avión: JFK a Ginebra
  - tren: Ginebra a Lausanne
- turista = datagrama
- segmento de transporte = enlace de comunicación
- modo de transporte = protocolo de la capa de enlace
- agente de viajes = algoritmo de enrutamiento

Servicios de la capa de enlace

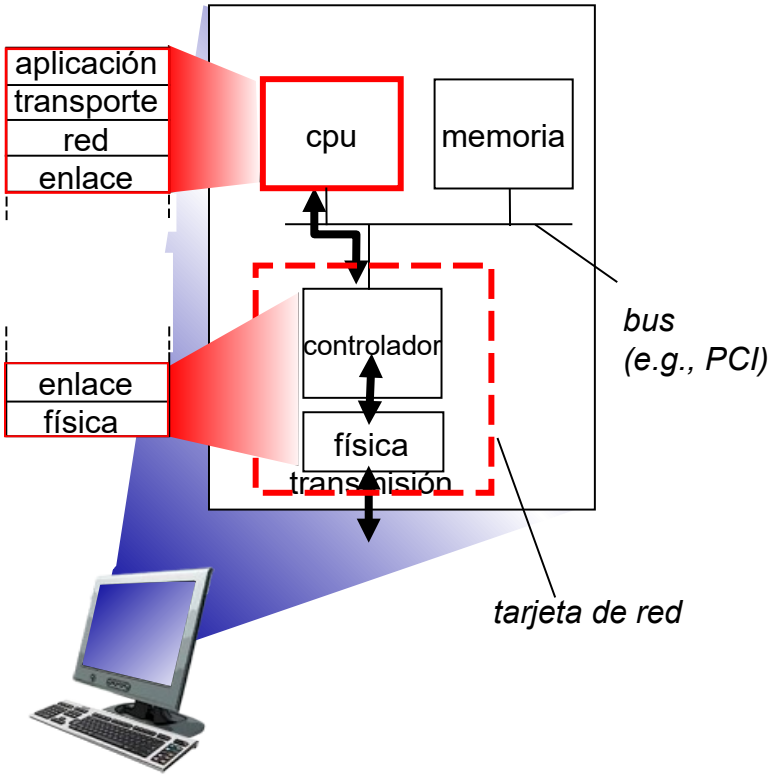
- entramado (framing), enlace de acceso:
  - esta capa encapsula el datagrama en la trama, agrega encabezado y lo envía a la siguiente capa
  - acceso al canal si es compartido
  - las direcciones "MAC" son usadas en los encabezados de la trama para identificar la fuente, el destino
    - diferente de la dirección IP!
- entrega confiable entre nodos adyacentes
  - ¡aprendimos cómo hacer esto ya (capítulo 3)!
  - rara vez se usa en enlaces de bajo error de bits (fibra, par trenzado)
  - enlaces inalámbricos: altas tasas de error
- P: ¿Por qué fiabilidad a nivel de enlace y también la de extremo a extremo?

Servicios de la capa de enlace (más)

- *control de flujo:*
  - estimulación entre los nodos de envío y recepción adyacentes
- *detección de errores:*
  - errores causados por la atenuación de la señal, ruido
  - el receptor detecta la presencia de errores:
    - avisa al emisor para su retransmisión, corrige o descarta la trama (frame)
- *corrección de errores:*
  - el receptor identifica y corrige errores de bit sin recurrir a la retransmisión
- *half-duplex y full-duplex*
  - con half-duplex, nodos en ambos extremos del enlace pueden transmitir, pero no a la misma vez

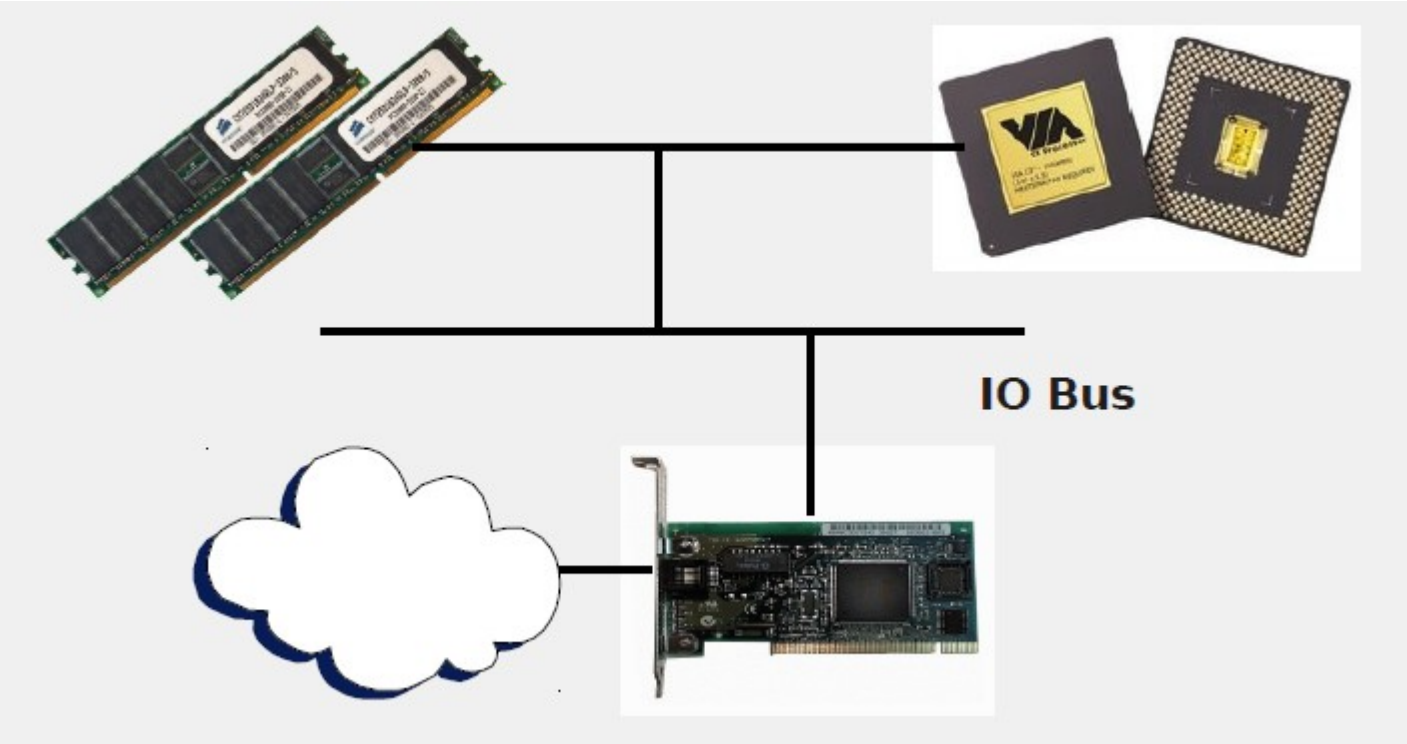
¿Dónde se implementa la capa de enlace?

- en cada uno de los equipos
- es implementada por un "adaptador" (aka *tarjeta de red* NIC) o en un chip
  - tarjeta de red ethernet card, tarjeta 802.11; chips para ethernet
  - Implementan las capas de enlace y la física
- está conectada a cada uno de los buses del sistema del equipo
- es la combinación de hardware, software y firmware



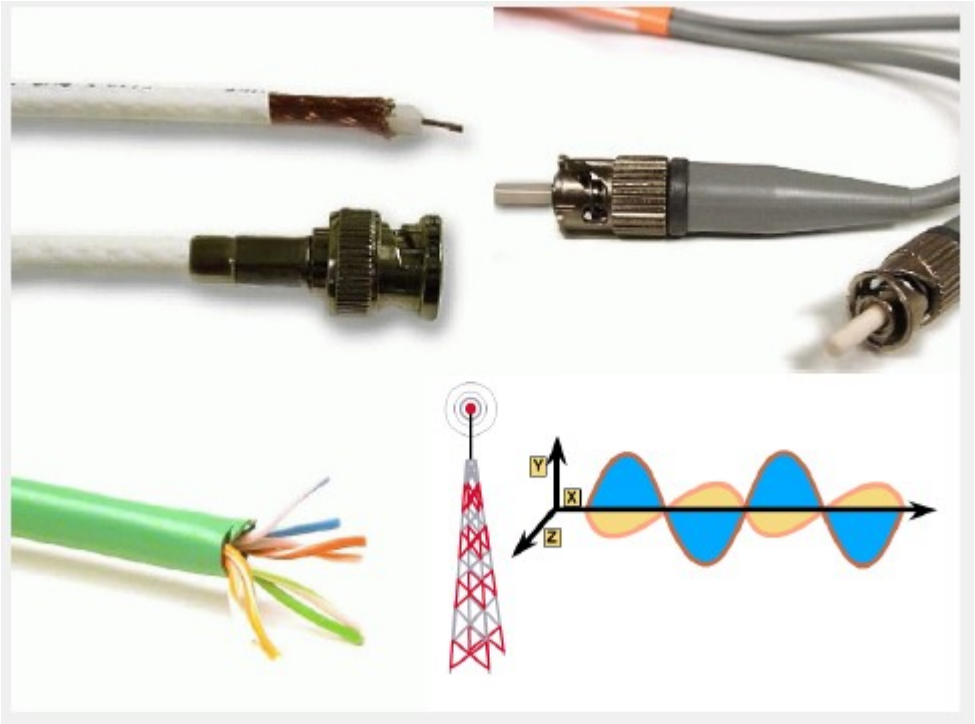
¿Dónde se implementa la capa de enlace?

- *Los enlaces son implementados:*
  - *A través de diversos tipos de tarjetas de red*

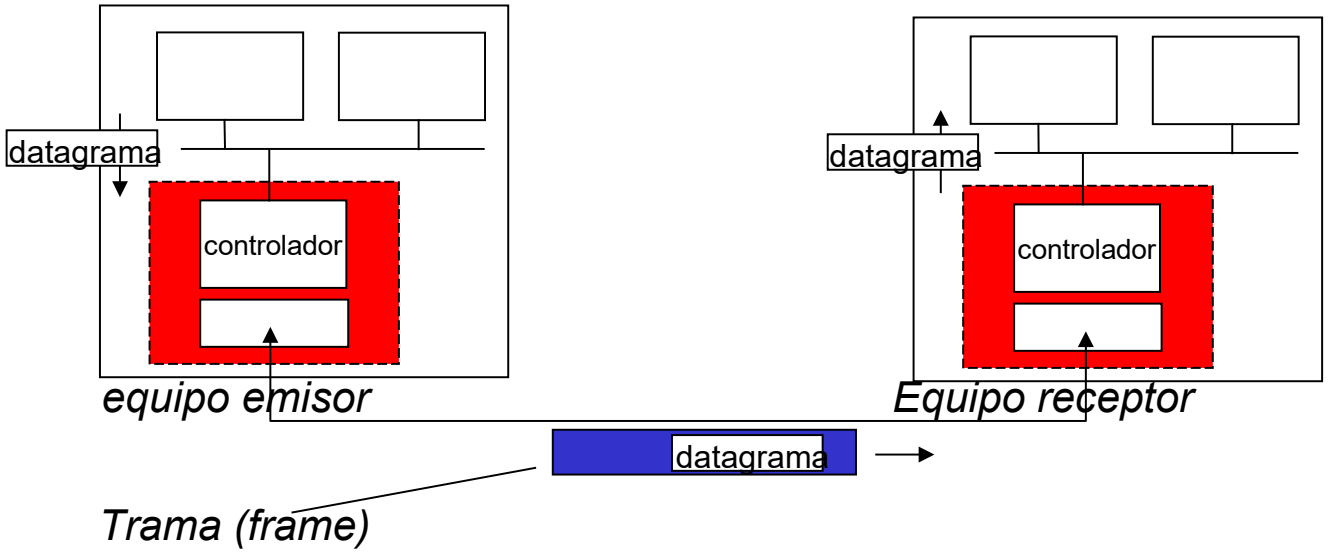


¿Dónde se implementa la capa de enlace?

- *Los enlaces son implementados:*
  - A través de diversos medios físicos



Comunicación entre adaptadores



- equipo emisor
  - encapsula el datagrama en una trama (frame)
  - agrega bits de chequeo de errores, rdt, control de flujos, etc.
- equipo receptor
  - busca errores, realiza control de flujos, rdt, etc
  - extrae datagramas y pasa a las capas superiores del lado receptor

Capa de enlace: ruta

5.1 introducción, servicios

5.2 detección de errores, corrección

5.3 protocolos de acceso múltiple

5.4 LANs

- direccionamiento, ARP
- ethernet
- switches
- VLANS

5.5 enlace de virtualización: MPLS

5.6 redes de centros de datos

5.7 un día en la vida de ena solicitud web

Detección de errores

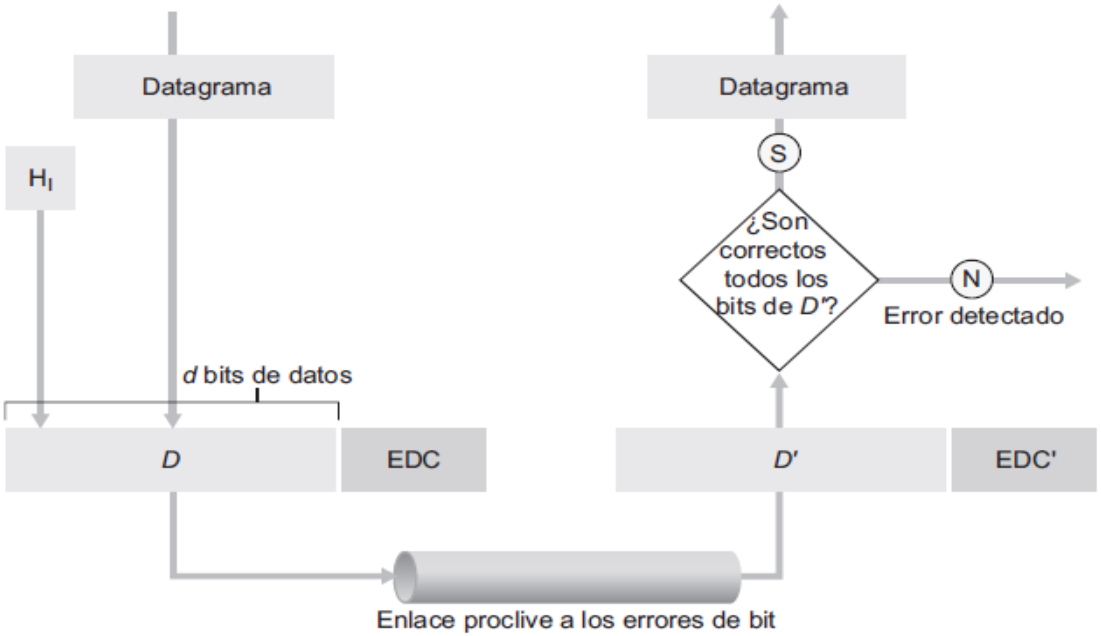
Examinemos ahora tres técnicas para detectar los errores en los datos transmitidos:

- comprobaciones de paridad (para ilustrar las ideas básicas que subyacen a las técnicas de detección y corrección de errores),
- métodos basados en suma de comprobación (que suelen utilizarse más en la capa de transporte) y
- códigos de redundancia cíclica (que normalmente se emplean más en el adaptador encargado en la capa de enlace).

Detección de errores

EDC= bits de detección y corrección de errrores (redundancia)
D= protección de datos por chequeo de errores, se incluye en la cabecera

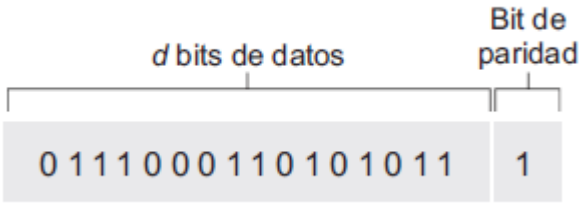
- OJO la detección de errores no es 100% confiable!
  - Los protocolos pueden pasar por alto algunos errores, pero es raro!
  - Campos más largos para la función de EDC producen una mejor detección y corrección de errores



Comprobación de paridad

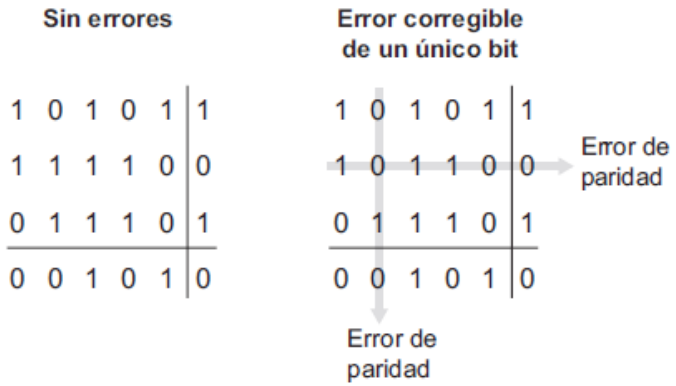
paridad de bit único:

- *detecta errores de un solo bit par o impar, sin ubicar cual*



paridad de bit bi-dimensional:

- detecta y corrige errores de un bit único



Suma de comprobación (revisión)

objetivo: detectar "errores" (e.g., bits volteados) en la transmisión de paquetes (nota: sólo usado en la capa de transporte) La suma de comprobación de Internet está basada en este enfoque: los bytes de datos se tratan como enteros de 16 bits y se suman. Entonces, se utiliza el complemento a 1 de esta suma para formar la suma de comprobación de Internet que se incluye en la cabecera del segmento.

emisor:

- trata a los segmentos como secuencias de 16-bit enteros
- realiza la suma de comprobación: se suman los contenidos de los segmentos
- el emisor pone el valor de la suma de comprobación en el campo correspondientes a suma de compración UDP

receptor:

- computa la suma de comprobación
- ¿La suma concuerda con el el campo de suma de compración recibido?
  - NO – detección de errores
  - YES – sin errores detectados Pero ojo que puede haber errores

Códigos de redundancia cíclica

- Una técnica detección de errores utilizada ampliamente en las redes de computadoras de hoy día esta basada en los códigos de comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check).

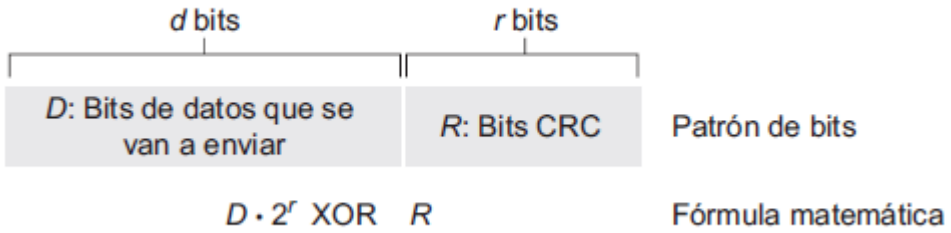
- Los códigos CRC también se conocen con el nombre de códigos polinómicos, dado que se puede ver la cadena de bits que hay que enviar como si fuera un polinomio cuyos coeficientes son los valores 0 y 1 de la cadena de bits, interpretándose las operaciones realizadas con la cadena de bits según la aritmética de polinomios.

Códigos de redundancia cíclica

- Es la herramienta mas poderosa para detección de errores
- Ve los datos como bits, D, como un entero binario
- Escoge un patrón r+1 (conocido cómo el generador), G
- Objetivo: escoge r CRC bits, R, de forma tal:
  - <D,R> son exactamente divisible por G (modulo 2)
  - El receptor conoce G, divide <D,R> por G. Si obtiene un resto diferente a cero: se ha detectado un error!
  - Puede detectar todos los errores menores de r+1 bits
- Es ampliamente utilizada en la práctica (Ethernet, 802.11 WiFi, ATM)

Códigos de redundancia cíclica

- Considera la secuencia de datos de d bits, D, que el nodo emisor quiere transmitir al nodo receptor. El emisor y el receptor tienen que acordar primero un patrón de r + 1 bits, G. Impondremos la condición de que el bit más significativo (el más a la izq.) de G sea 1.



- Para la secuencia de datos, D, el emisor seleccionará r bits adicionales, R, y se los añadirá a D, de modo que el patrón de d + r bits resultante (interpretado como un número binario) sea exactamente divisible por G (es decir, no tenga ningún resto) utilizando aritmética módulo 2. El proceso de comprobación de errores de CRC es muy simple: el receptor divide los d + r bits recibidos entre G. Si el resto es distinto de cero, el receptor sabrá que se ha producido error; sino, se aceptarán los datos como correctos.

Capa de enlace: ruta

5.1 introducción, servicios

5.2 detección de errores, corrección

5.3 protocolos de acceso múltiple

5.4 LANs

- direccionamiento, ARP
- ethernet
- switches
- VLANS

5.5 enlace de virtualización: MPLS

5.6 redes de centros de datos

5.7 un día en la vida de ena solicitud web

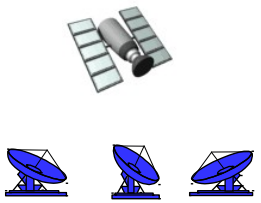
Protocolos de acceso múltiple

2 tipos de "enlaces":

- punto-a-punto
  - PPP para acceso dial-up
  - enlace punto-a-punto entre switchs ethernet
- *Difusión (broadcast) cableado o medio compartido*
  - El antiguo Ethernet
  - upstream HFC
  - 802.11 LAN inalámbrica

Cableado compartido (Ethernet)

Radio frecuencia compartida (e.g., 802.11 WiFi)



Radio frecuencia compartida (satellite)

Humanos en una fiesta (comparten el medio, aire)

Protocolos de acceso múltiple

- Un solo canal de difusión compartido
- 2 o más nodos de transmisión simultáneos: interferencia
  - *colisión* si un nodo recibe 2 o más señales a la misma vez

protocolos de acceso múltiple

- Algoritmos distribuidos que determinan cómo se comparte un canal, i.e., determina cuando un nodo puede transmitir
- La comunicación sobre cómo compartir el canal también viaja por el canal!
  - No hay coordinación del canal fuera de él

Un protocolo ideal de acceso múltiple

dado: un canal de difusión con un tasa de R bps

queremos:

1. cuando un nodo quiere transmitir, puede hacerlo a la tasa R.
2. cuando M nodos quieren transmitir, cada uno puede hacerlo a tasa promedio de R/M
3. totalmente descentralizado:
   - No hay un nodo especial para coordinar las transmisiones
   - No hay sincronización de relojes o slots
4. simple

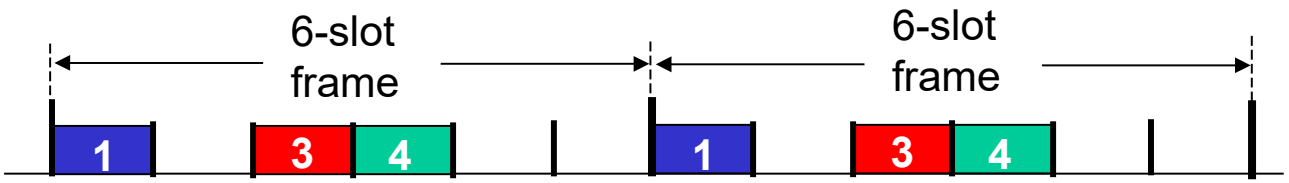
Protocolos MAC: taxonomía

- *particionamiento del canal*
  - divide el canal en "piezas" más pequeñas (slots de tiempo, frecuencia, código)
  - allocate piece to node for exclusive use
- *protocolos de acceso aleatorio*
  - canal sin divisiones, permite colisiones
  - "recuperación" ante colisiones
- *"toma de turnos"*
  - Los nodos toman turnos, pero los nodos con más datos que enviar pueden tomar turnos más largos

Protocolo MAC de particionamiento del canal: TDMA

TDMA: multiplexación por división en el tiempo

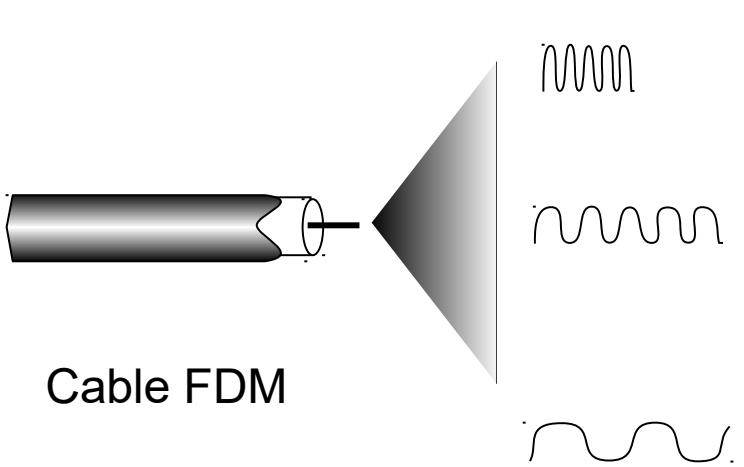
- acceso al canal por "rondas"
- cada nodo obtiene una tasa de transmisión dedicada igual a los demás durante cada ronda
- un nodo siempre tiene que esperar a que le llegue el turno dentro de la secuencia de transmisión
- los turnos no utilizados quedan inactivos
- ejemplo: 6-estaciones en la LAN, 1,3,4 tienen un paquete, pero 2,5,6 están inactivos

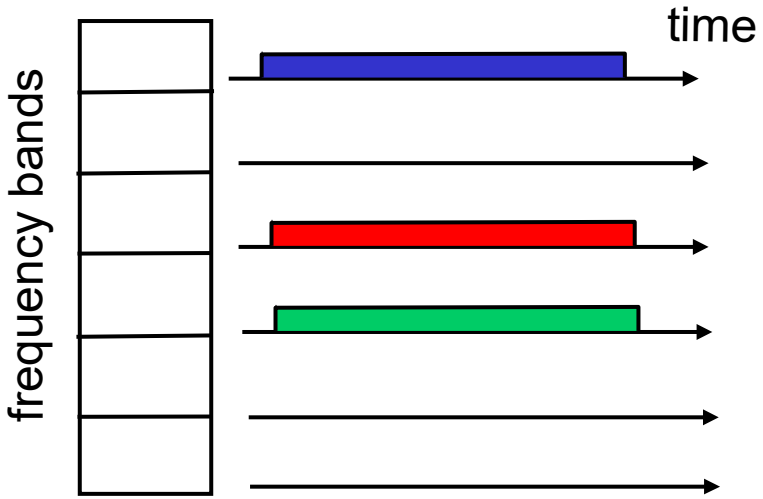


Protocolo MAC de particionamiento del canal: FDMA

FDMA: multiplexación por división de frecuencia

- el espectro del canal se divide en bandas de frecuencia
- a cada estación se le asigna una banda de frecuencia fija
- el tiempo en el que no se realiza transmisión en esa banda queda inactivo
- ejemplo: 6-estaciones en la LAN, 1,3,4 tienen un paquete, pero las bandas de frecuencia de 2,5,6 están inactivos





Protocolos de acceso aleatorio

- cuando un nodo tiene un paquete que enviar
  - transmite a la tasa máxima R que le permite el canal
  - no existe una coordinación *a priori* entre nodos
- 2 o más nodos transmitiendo ➜ "colisión",
- el protocolo de acceso aleatorio especifica:
  - cómo detectar colisiones
  - cómo recuperarse de las colisiones (e.g., via transmisiones con retardo)
- ejemplos de protocolos de acceso aleatorio:
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

ALOHA con particiones

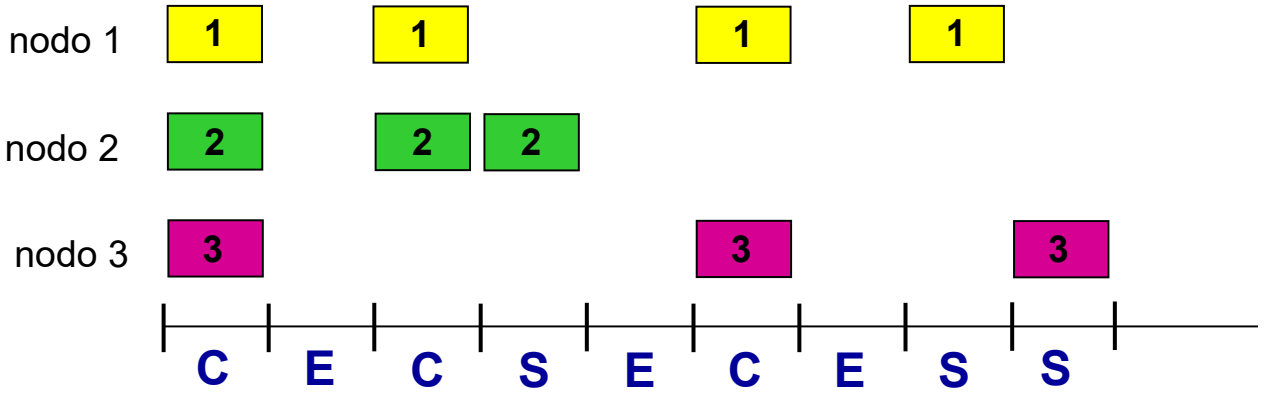
suposiciones:

- todas las tramas son del mismo tamaño
- el tiempo se divide en particionamientos (slots) del mismo tamaño (tiempo en transmitir 1 trama)
- los nodos comienzan a transmitir sólo al comienzo del particionamiento (slot) de tiempo
- los nodos están sincronizados
- si 2 o más nodos transmiten en el mismo particionamiento, todos los nodos detectarán la colisión

operación:

- cuando un nodo obtiene una trama nueva, la transmite en el siguiente particionamiento (slot)
  - ***Si no hay colisión:*** el nodo puede enviar una nueva trama en el siguiente particionamiento de tiempo
  - ***Si hay colisión:*** el nodo retransmite la trama en cada particionamiento subsecuenta con la probabilidad de p de éxito

ALOHA con particiones



Pros:

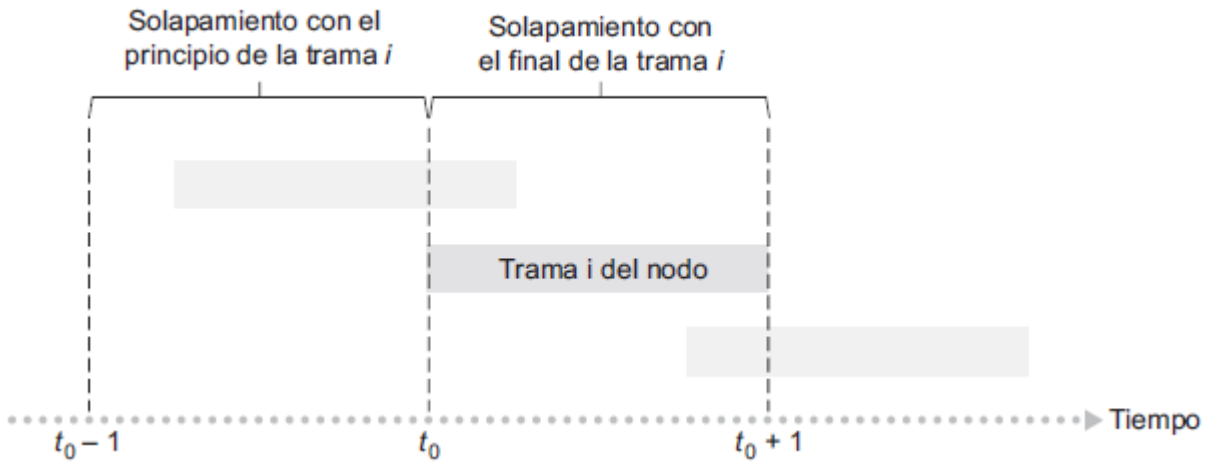
- un sólo nodo activo puede transmitir de forma continua a máxima velocidad
- es altamente descentralizado: sólo los particionamientos en los nodos tiene que sincronizarse
- simple

Contras:

- colisiones, desperdicios de particionamientos de tiempo
- particionamientos de tiempo inactivos
- los nodos deben detectar la colisión en menos tiempo que la transmisión del paquete
- sincronización de relojes

ALOHA puro (sin particionamientos)

- aloha sin particionamientos: es más simple, sin sincronización
- cuando la primera trama llega
  - se transmite inmediatamente
- la probabilidad de colisión se incrementa:
  - una trama es enviada al tiempo t_0 colisiona con otra trama enviada en $[t_0-1, t_0+1]$



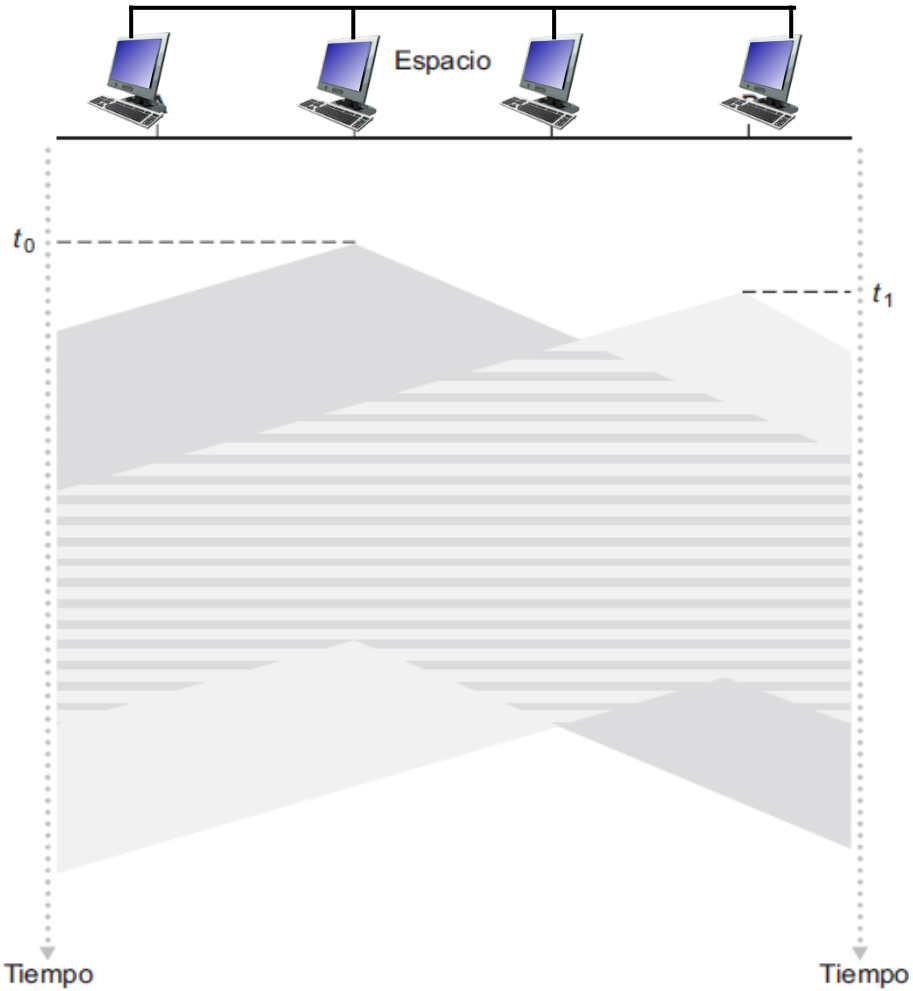
Acceso múltiple con sondeo de portadora (CSMA, Carrier Sense Multiple Access)

CSMA: escucha antes de transmitir:

- Si el canal está libre: transmite la trama completa
- Si el canal está en uso, difiere la transmisión
- Analogía con los humanos: no interrumpas a los demás!

Colisiones de CSMA

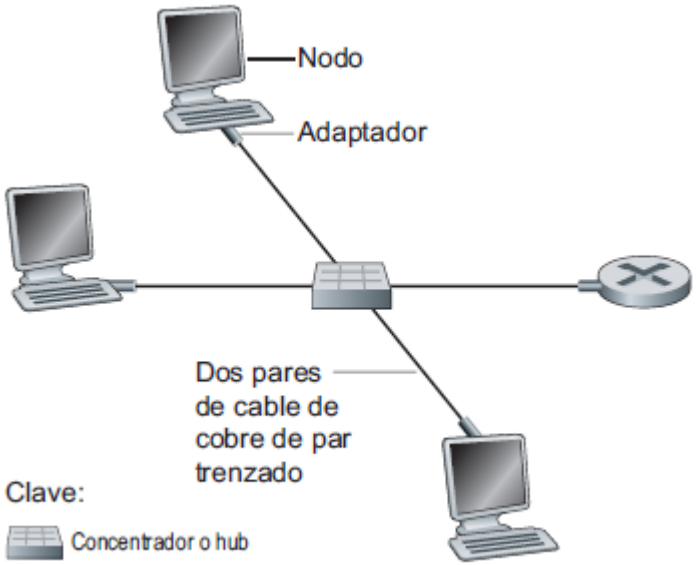
- Las colisiones pueden ocurrir: la propagación de los retardos significa que 2 nodos pueden no oír las transmisiones de los demás
- colisión: el tiempo entero de transmisión del paquete se pierde
  - distancia & propagación del retardo juegan un rol determinante en la determinación de la probabilidad de colisión



CSMA/CD (con detección de colisiones)

CSMA/CD en la vida real:

Cuando los nodos están interconectados mediante un concentrador (en oposición a un conmutador de la capa de enlace), como se muestra en la Figura, la LAN Ethernet es una auténtica LAN de difusión; es decir, cuando un adaptador transmite una trama, todos los adaptadores de la LAN reciben esa trama. Dado que Ethernet puede emplear la comunicación por difusión, necesita un protocolo de acceso múltiple. Ethernet utiliza el famoso protocolo de acceso múltiple CSMA/CD.



CSMA/CD (con detección de colisiones)

CSMA/CD:

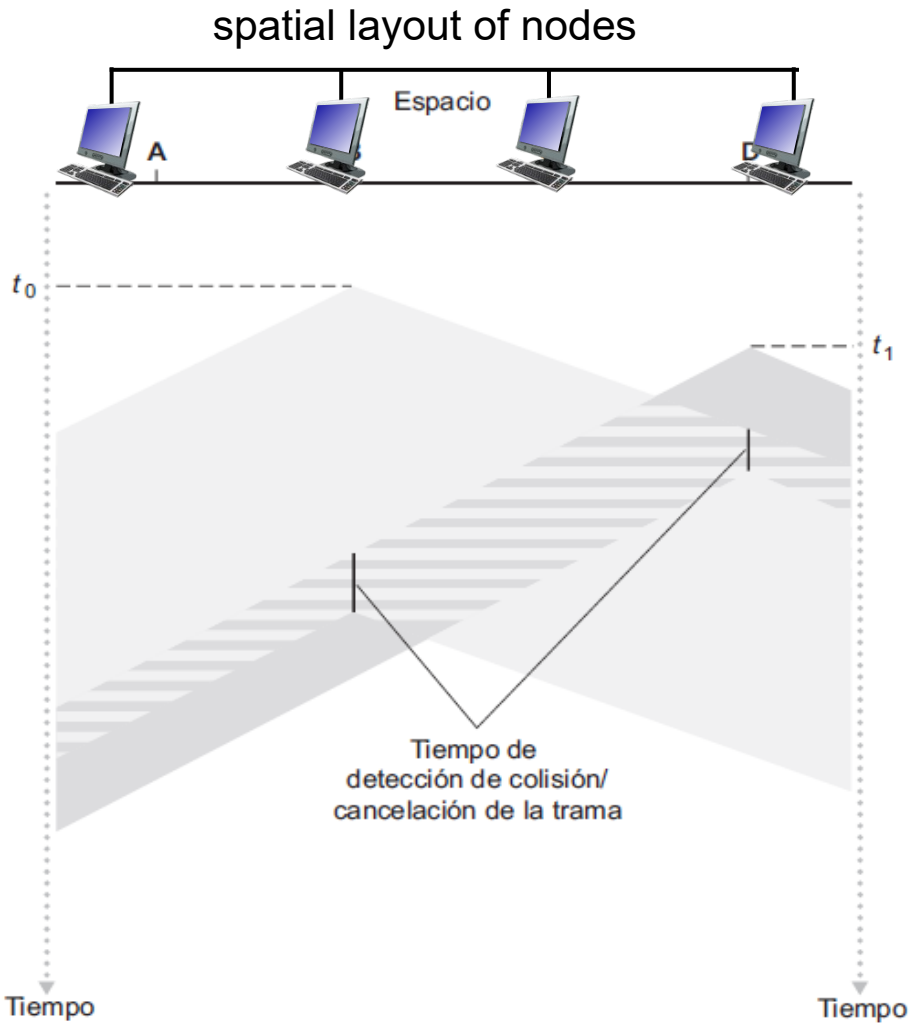
1) Un adaptador puede comenzar a transmitir en cualquier instante; es decir, no existe el concepto de partición de tiempo.
2) Un adaptador nunca transmite una trama cuando detecta que algún otro adaptador está transmitiendo; es decir, utiliza un mecanismo de sondeo de portadora.
3) Un adaptador que está transmitiendo aborta su transmisión tan pronto como detecta que otro adaptador también está transmitiendo; es decir, utiliza un mecanismo de detección de colisiones.
4) Antes de intentar llevar a cabo 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.

CSMA/CD (con detección de colisiones)

Algoritmo de CSMA/CD:

1) El adaptador obtiene un datagrama de la capa de red, prepara una trama Ethernet y la coloca en un buffer del adaptador.
2) Si el adaptador detecta que el canal está inactivo (es decir, durante 96 periodos de bit el adaptador no recibe intensidad de señal procedente del canal), comienza a transmitir la trama. Si el adaptador detecta que el canal está ocupado, espera hasta comprobar que no hay intensidad de señal (más otros 96 periodos de bit) y luego comienza a transmitir la trama.
3) Mientras está transmitiendo, el adaptador monitoriza la presencia de señales procedentes de otros adaptadores. Si el adaptador transmite la trama completa sin detectar ninguna señal procedente de otros adaptadores, concluye que ha terminado su trabajo con esa trama.
4) Si el adaptador detecta intensidad de señal procedente de otros adaptadores mientras está transmitiendo, deja de transmitir su trama y transmite una señal de interferencia (jam) de 48 bits.
5) Después de abortar la transmisión de la trama (es decir, de transmitir la señal de interferencia), el adaptador entra en la fase de espera exponencial (backoff exponencial). Específicamente, a la hora de transmitir una determinada trama, después de experimentar la n-ésima colisión para esa trama, el adaptador selecciona un valor aleatorio para K del conjunto {0,1,2, . . . , 2m – 1}, donde m

CSMA/CD (con detección de colisiones)



Protocolos de "toma de turnos"

Motivación!

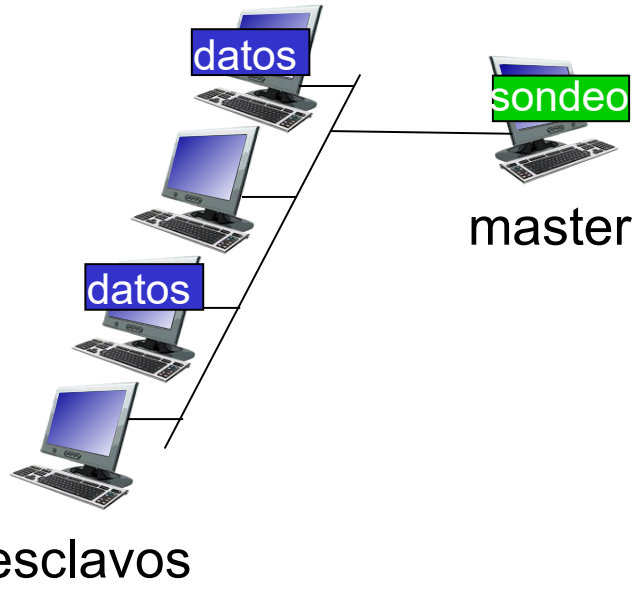
- 2 propiedades deseables de un protocolo de acceso múltiple son:
  1) Cuando sólo haya un nodo activo, éste tendrá una tasa de transferencia de R bps
  2) Cuando haya M nodos activos, entonces cada nodo activo dispondrá de una tasa de transferencia de aproximadamente R/M bps.

- Los protocolos ALOHA y CSMA presentan la primera de las propiedades,pero no la segunda.
- Esto ha servido de motivación para que una serie de investigadores creen otra clase de protocolos MAC

"Toma de turnos": protocolo de sondeo (polling)

sondeo:

- Este protocolo requiere que se designe a uno de los nodos como nodo **maestro**.
- El nodo maestro sondea a cada uno de los otros nodos a la manera de turno rotatorio (round robin).
- En particular, el nodo maestro envía primero un mensaje al nodo 1, diciéndole que puede transmitir hasta un cierto número máximo de tramas
- El protocolo de sondeo elimina las colisiones y las particiones vacías que infectan los protocolos de acceso aleatorio. Esto permite que el mecanismo de sondeo consiga una eficiencia mucho mayor
- El protocolo 802.15 y el protocolo Bluetooth que estudiaremos en la Sección 6.3 son ejemplos de protocolos de sondeo.

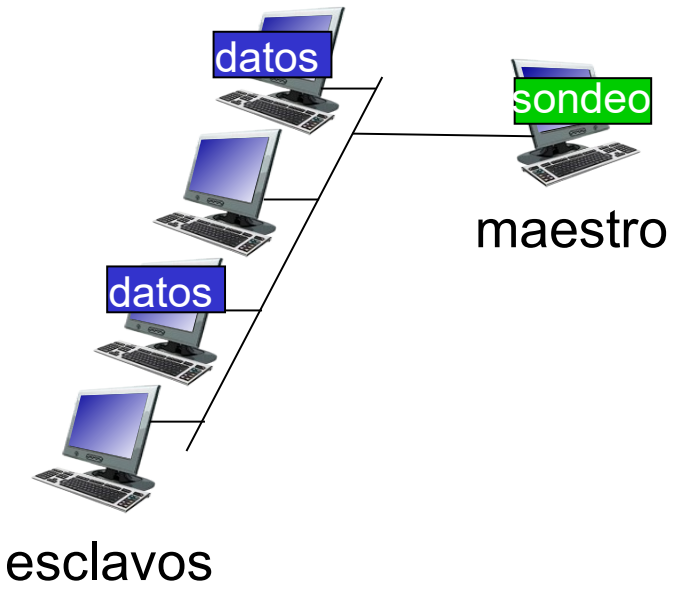


802.15 y Bluetooth son ejemplos de la implementación exitosa de protocolos de sondeo.

"Toma de turnos": protocolo de sondeo (polling)

desventajas:

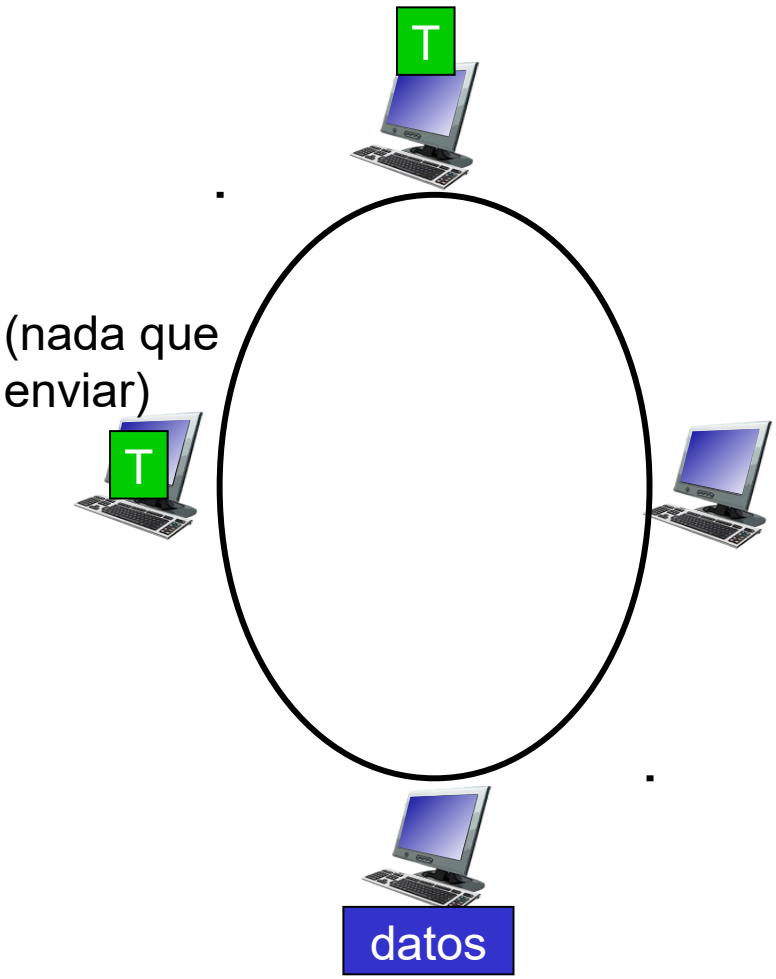
- el protocolo introduce un retardo de sondeo: el intervalo de tiempo requerido para indicarle a un nodo que puede transmitir.
  - Por ejemplo, si sólo hay un nodo activo, entonces el nodo transmitirá a una velocidad menor que R bps, ya que el nodo maestro deberá sondear a cada uno de los nodos inactivos por turno cada vez que el nodo activo haya terminado de enviar su número máximo de tramas.
- El riesgo de punto único de falla! Si falla el nodo maestro, queda inoperativa la red



"Toma de turnos" protocolo de paso de testigo

Paso del tesigo (token passing):

- El *testigo de control* se pasa de un nodo a otro secuencialmente.
- No hay nodos maestros, en su lugar hay una trama pequeña, llamada testigo
- Cuando un nodo obtiene el testigo, lo entrega sino tiene nada que enviar y lo retiene mientras envia sus tramas una tras otra hasta que llegue al max. de tramas por turno o termine con los que tenía por enviar



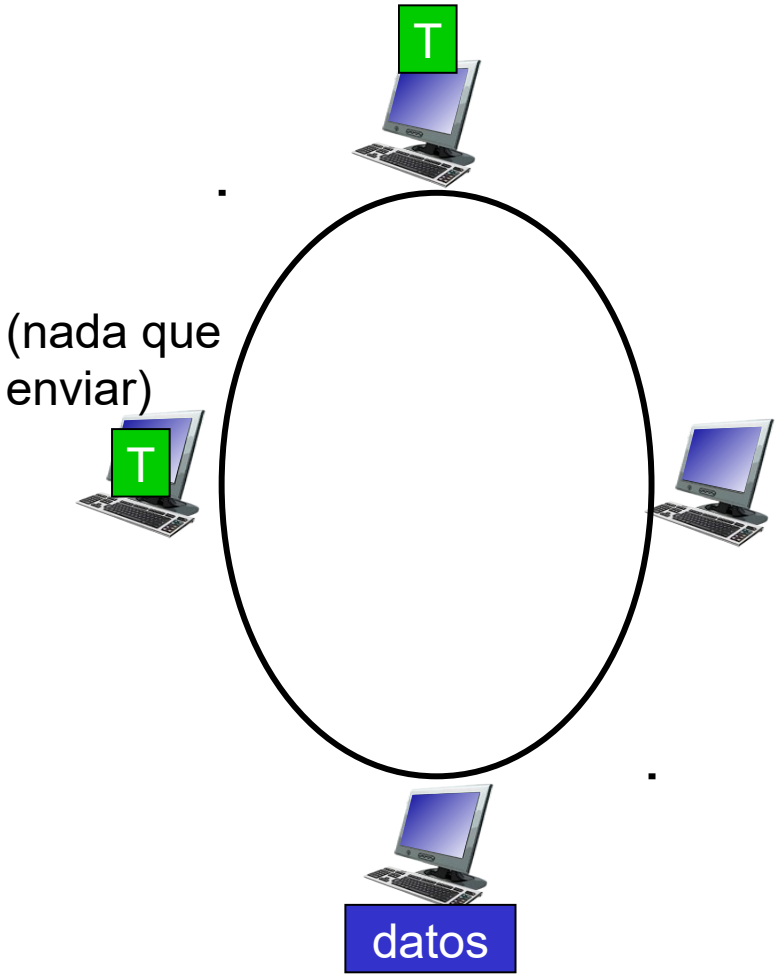
"Toma de turnos" protocolo de paso de testigo

desventajas:

- Un punto único de falla (el testigo)
- Latencia
- Desborde del testigo

ejemplos:

- FDDI
- 802.5



Resumen de los protocolos MAC

- *Partición del canal,* por tiempo, frecuencia o código
  - División por tiempo, división por frecuencia
- *Acceso aleatorio* (dinámico),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: fácil en algunas tecnologías (cableadas), duro en otras (inalámbrica)
  - CSMA/CD usado en ethernet
  - CSMA/CA usado en 802.11
- *"Toma de turnos"*
  - Sondeo desde un nodo central (maestros, esclavos), "Toma de turnos" protocolo de paso de testigo.
  - bluetooth, FDDI, token ring

Capa de enlace: ruta

5.1 introducción, servicios
5.2 detección de errores, corrección
5.3 protocolos de acceso múltiple
5.4 LANs
- direccionamiento, ARP
- ethernet
- switches
- VLANS

5.5 enlace de virtualización: MPLS
5.6 redes de centros de datos
5.7 un día en la vida de ena solicitud web

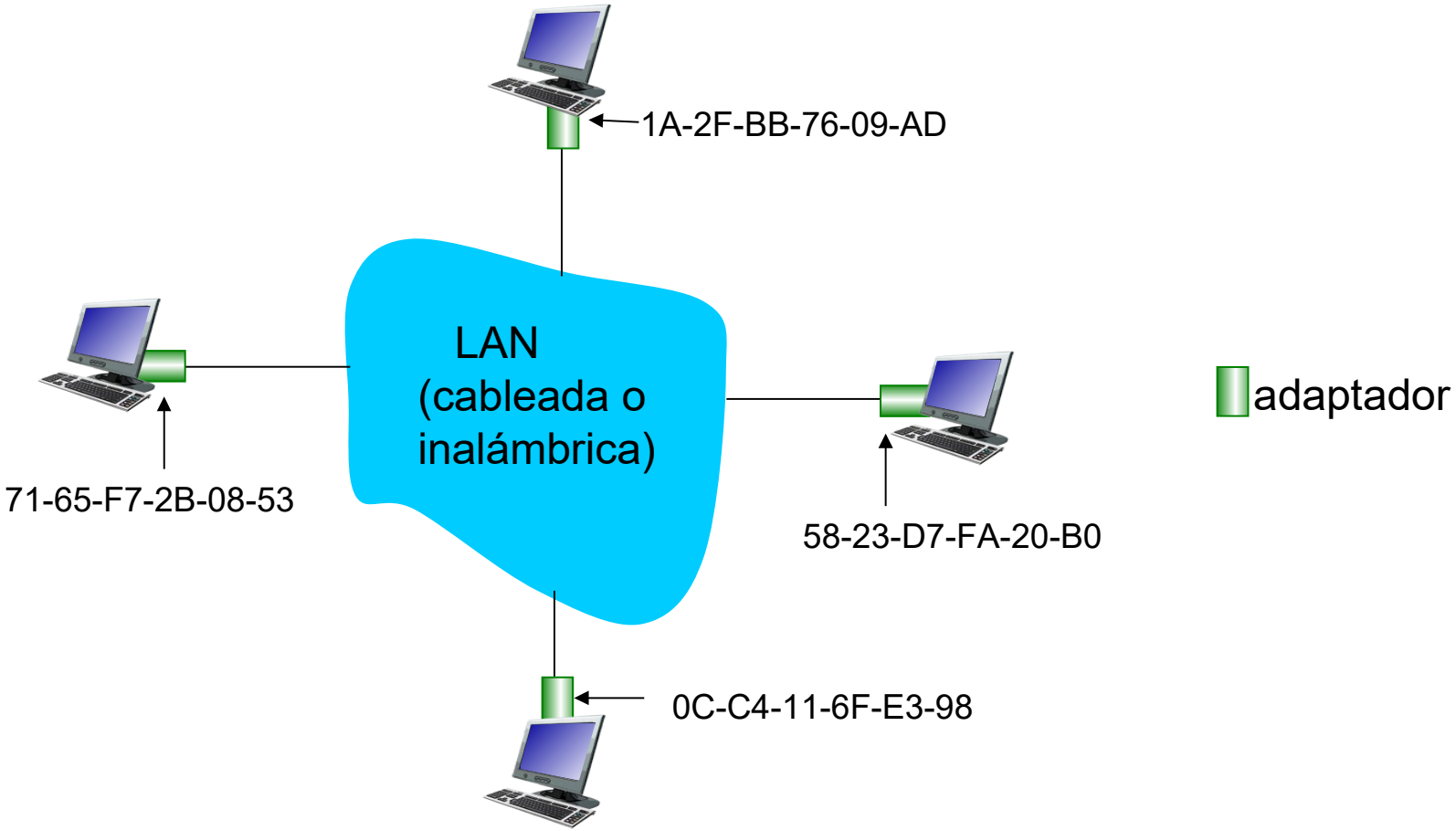
Dirección MAC y ARP

- Direcciones IP de 32-bit :
  - *Dirección a nivel de capa de red para la interfaz*
  - Usada por la capa 3 (capa de red o internet) para el envío de paquetes
- Dirección MAC (o LAN o física o Ethernet):
  - función: *usarla 'localmente" para llevar una trama de una interfaz física a otra "físicamente conectadas" (en la misma red, si hablamos desde el punto de vista de direccionamiento IP)*
  - La dirección MAC tiene 48 bit (para casi todoas las LAN) quemada en el NIC del ROM, aunque a veces se puede configurar vía software
  - e.g.: 1A-2F-BB-76-09-AD

Utiliza notación hexadecimal (base 16)
cada "número" representa 4 bits

Direcciones LAN y ARP

Cada adaptador LAN tiene una única dirección LAN



Direccionamiento LAN (más)

- La distribución de direccionamiento MAC es administrado por la IEEE
- Los productores de interfaces de red compran prorciones de direccionamiento MAC (para asegurar que son únicas)
- analogía:
  - dirección MAC: número de seguro social
  - dirección IP: dirección postal
- La dirección MAC son planas ➜ portables
  - Puedes mover una MAC de una LAN a otra sin problemas
- Las direcciones IP son jerárquicas y nos portables
  - La dirección IP depende de la subred a la cual está conectado el nodo

ARP: protocolo de resolución de direcciones

pregunta: cómo determinar la dirección MAC de una interfaz si sabemos la dirección IP?

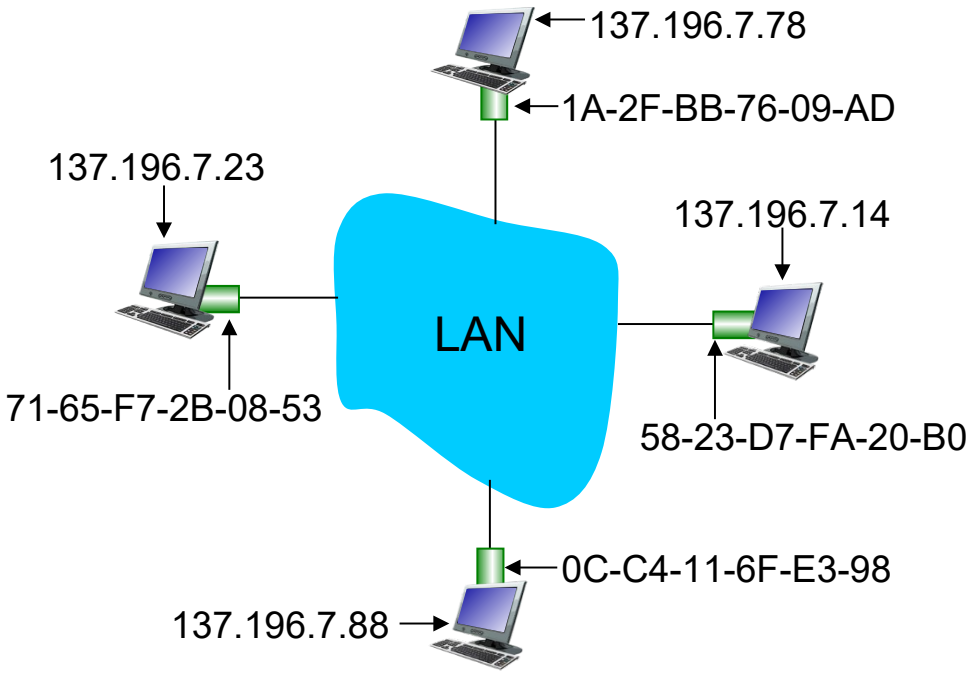


Tabla ARP: cada nodo IP (equipo, enrutador) en la LAN tiene una tabla

- Mapeando dirección IP/MAC para los nodos LAN:

  < dirección IP; dirección MAC; TTL>

- TTL (Time To Live): tiempo en el cual un mapeo de una dirección será olvidada (usualmente 20 min)

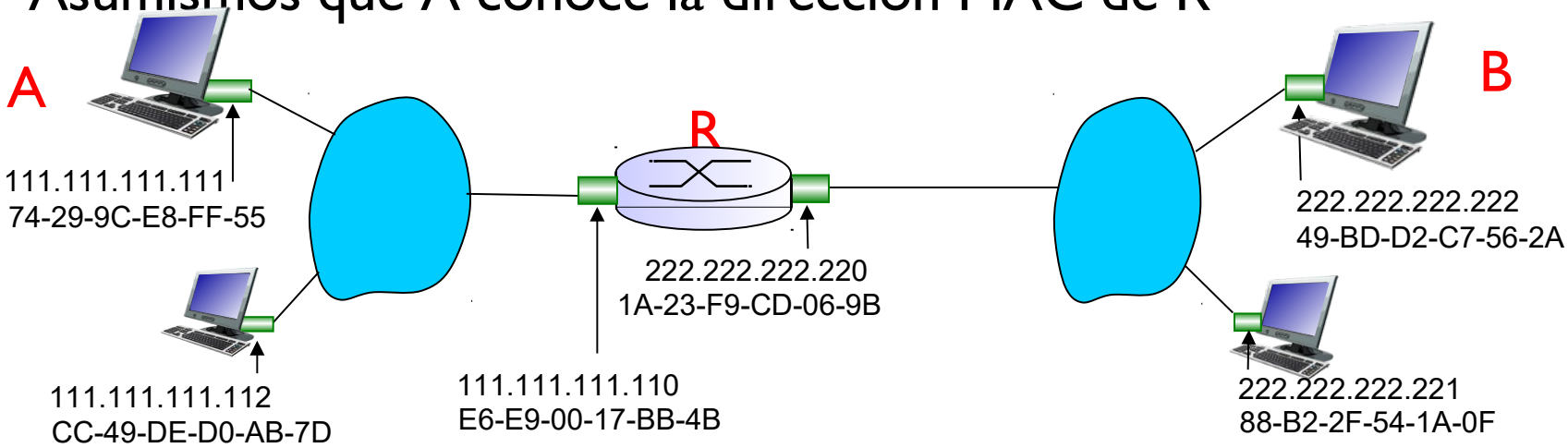
Protocolo ARP: misma LAN

- A quiere enviar un datagrama a B
  - B's MAC la dirección no está en la tabla ARP de A
- A difunde una consulta de la dirección con un paquete ARP, este paquete contiene la dirección IP de B
  - Dirección dest MAC = FF-FF-FF-FF-FF-FF
  - Todos los nodos en la LAN reciben la solicitud de la consulta
- B recibe el paquete ARP, y le responde a A con su dirección MAC
- Un cache (guarda) la pareja dirección IP-MAC en su tabla ARP hasta que la información se haga obsoleta
  - Estado suave: la información a la que se le acaba el tiempo se borra a menos que se refresque
- ARP es "plug-and-play":
  - Los nodos crean su tabla ARP sin intervención del administrador del equipo o de red

Direccionamiento: enrutando hacia otra LAN

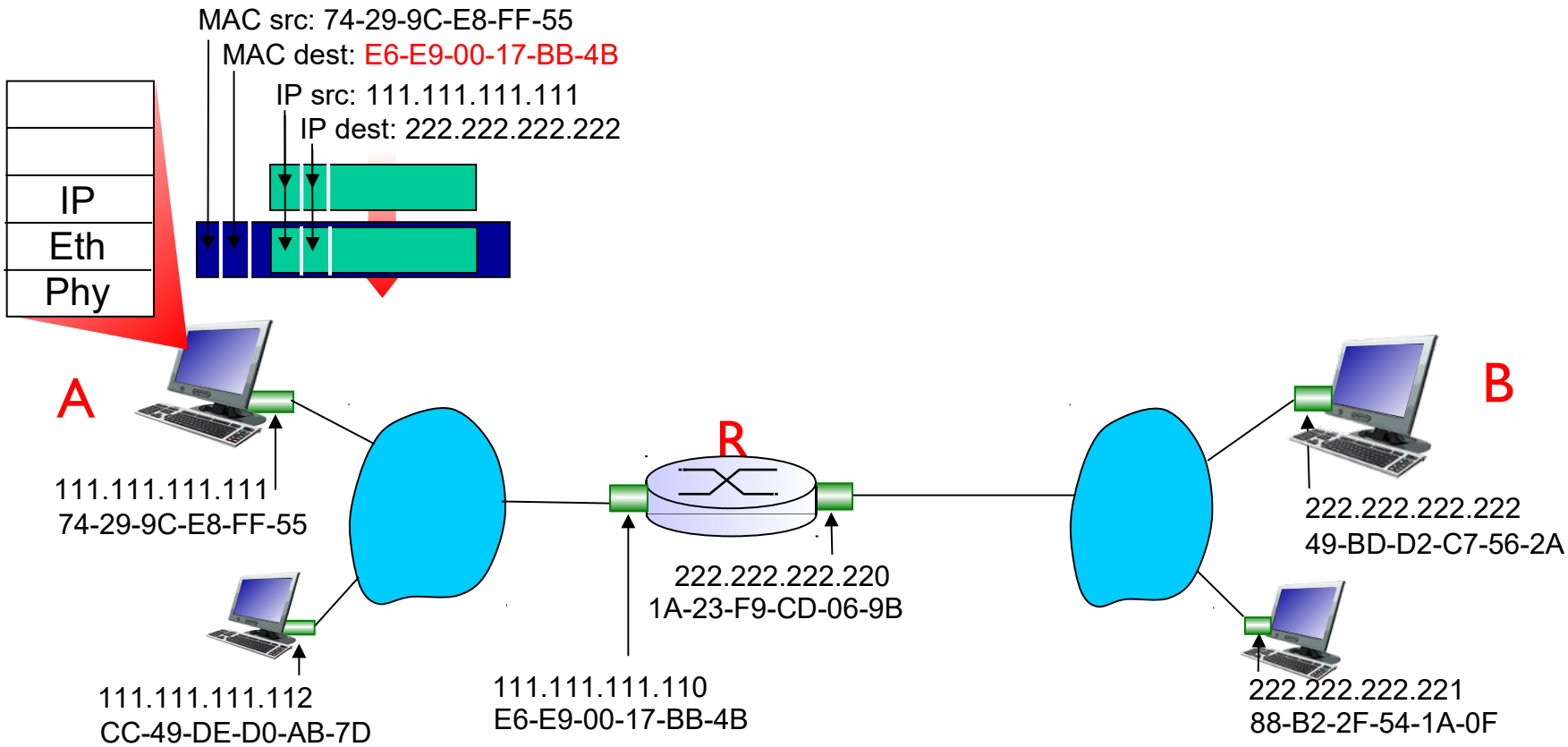
Veamos cómo el datagrama A es enviado a B vía R

- Ojo con el direccionamiento – a nivel IP (datagrama) y en la capa de enlace con dirección MAC (trama)
- Asumimos que A conoce la dirección IP de B
- Asumimos que conoce la dirección IP del primero salto al enrutador, R
- Asumismos que A conoce la dirección MAC de R



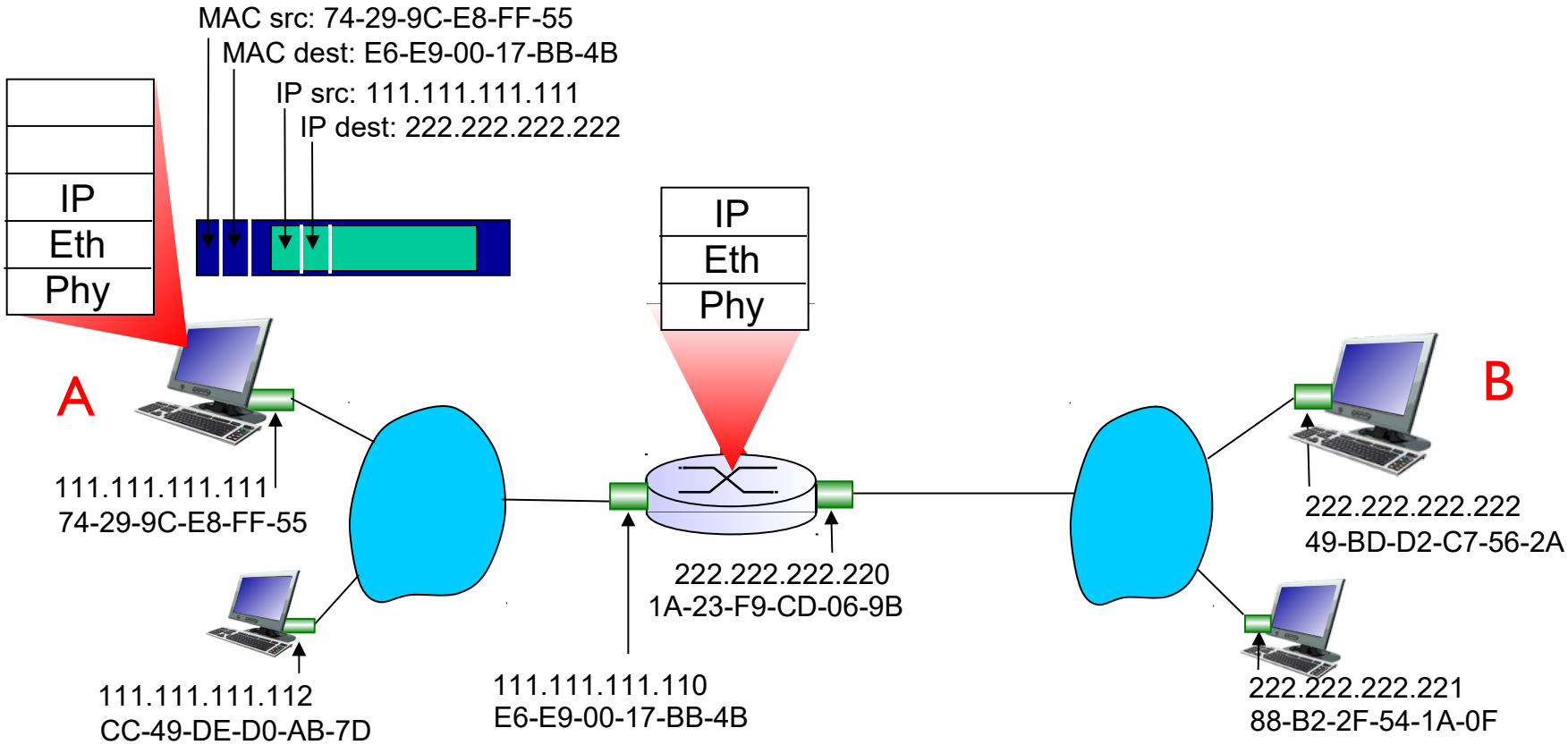
Direccionamiento: enrutando hacia otra LAN

- A crea un datagrama IP con la dirección IP fuente A, y destino B
- A crea una trama de capa de enlace con la dirección MAC R cómo destino, la trama contiene el datagrama IP A-B



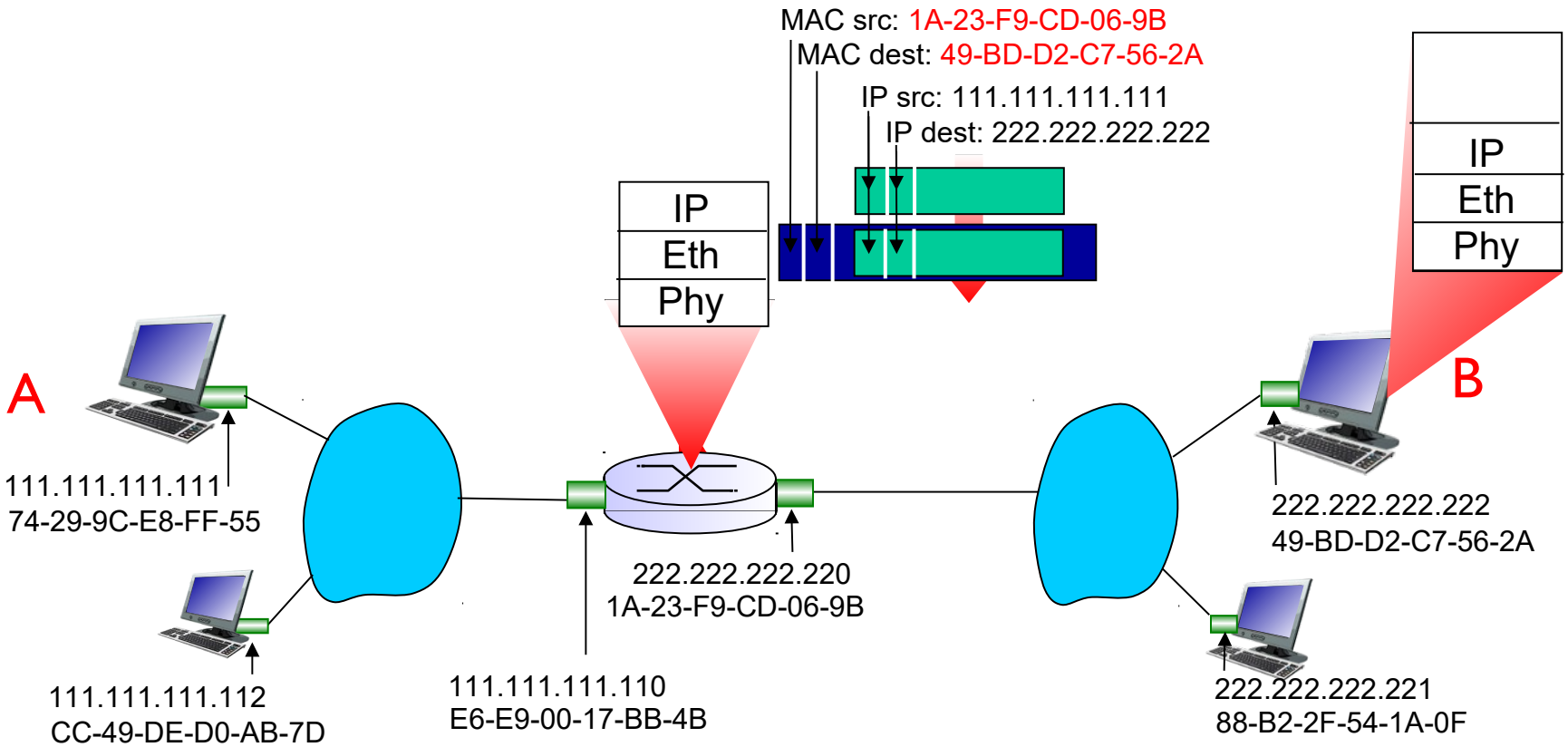
Direccionamiento: enrutando hacia otra LAN

- Se envia una trama de A a R
- R recibe la trama, se elimina el datagrama, y se pasa al siguiente nivel IP



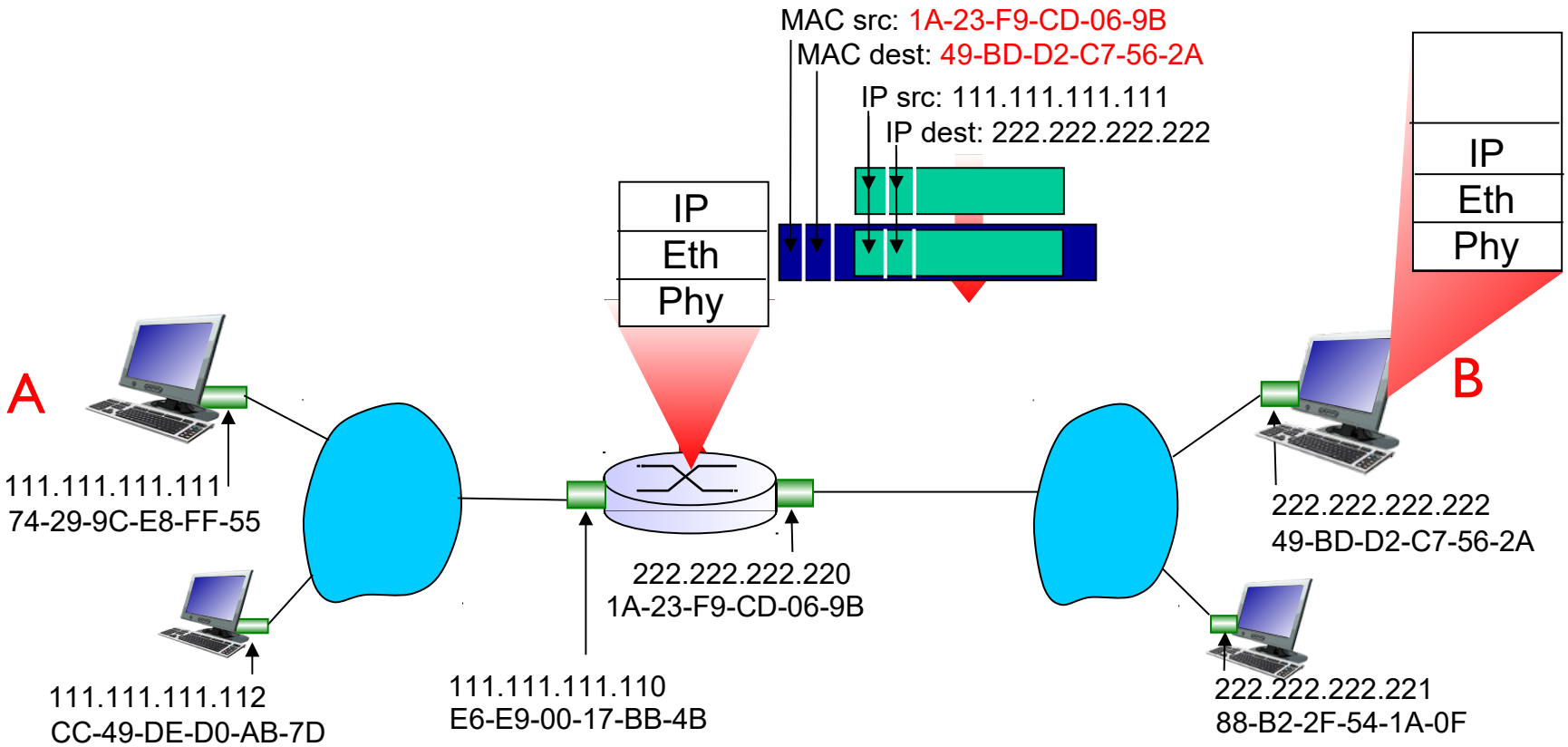
Direccionamiento: enrutando hacia otra LAN

- R redirige el datagrama con IP fuente A, a su destino B
- R crea un trama de capa de enlace con la dirección MAC de como dirección destino, la trama contiene el datagrama IP A-B



Direccionamiento: enrutando hacia otra LAN

- R redirige el datagrama con IP fuente A, a su destino B
- R crea un trama de capa de enlace con la dirección MAC de como dirección destino, la trama contiene el datagrama IP A-B



Direccionamiento: enrutando hacia otra LAN

- R redirige el datagrama con IP fuente A, a su destino B
- R crea un trama de capa de enlace con la dirección MAC de como dirección destino, la trama contiene el datagrama IP A-B