Redes de datos

Capa de enlace

Facultad de Ingeniería – Universidad de la República

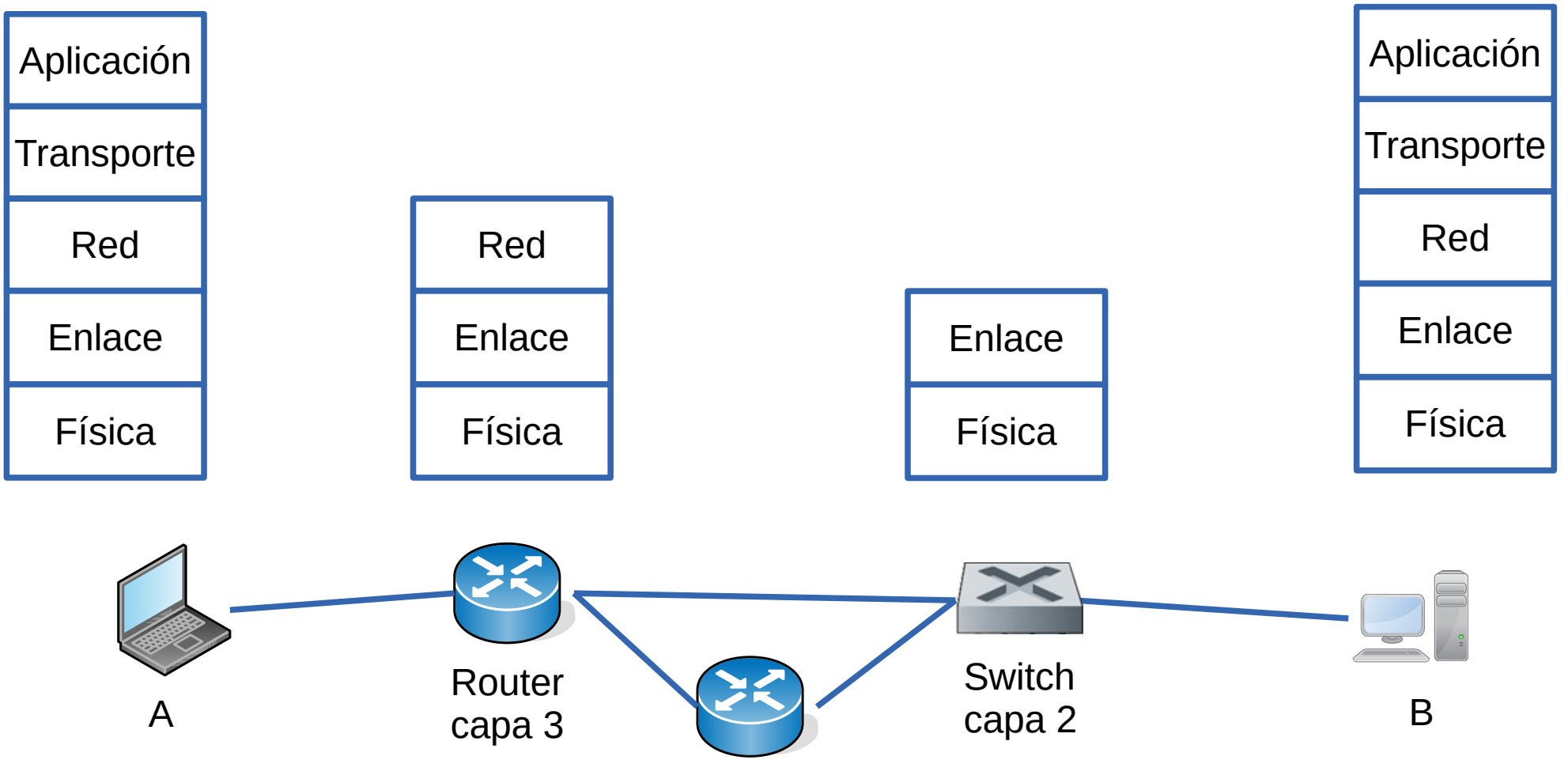
2024

Agenda

- Conceptos de capa de enlace
  - Objetivo y funciones de la capa de enlace
  - Entramado
  - Detección y corrección de errores
  - Servicios confiables
- Ejemplos de protocolos punto a punto
- Protocolos de acceso a medios compartidos
  - Protocolos para compartir el canal
- Redes de área local cableadas
  - 802.3 y su evolución
  - Redes con switches
  - Vlans
- Redes de área local inalámbricas
- Networking en el datacenter

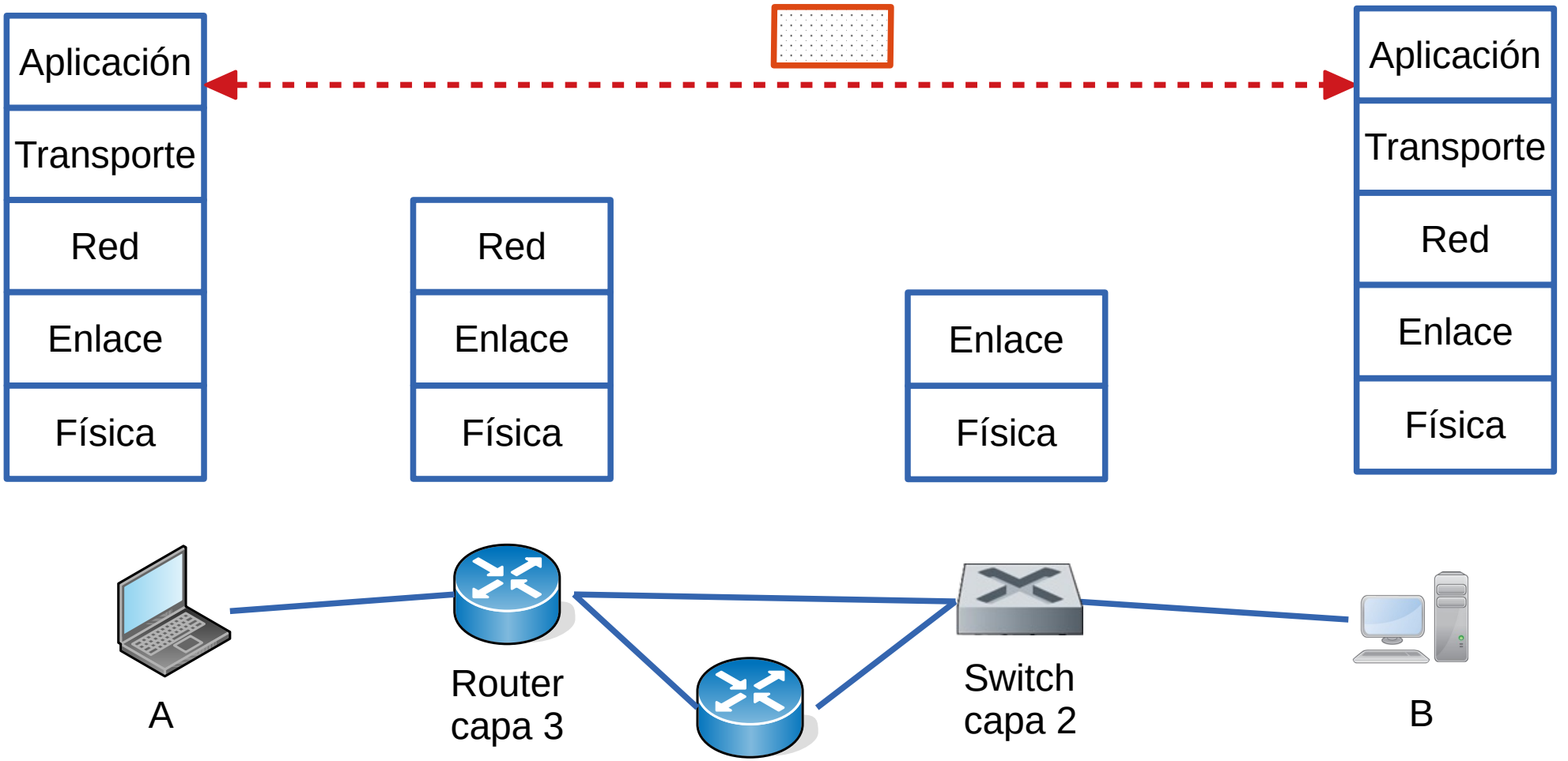
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



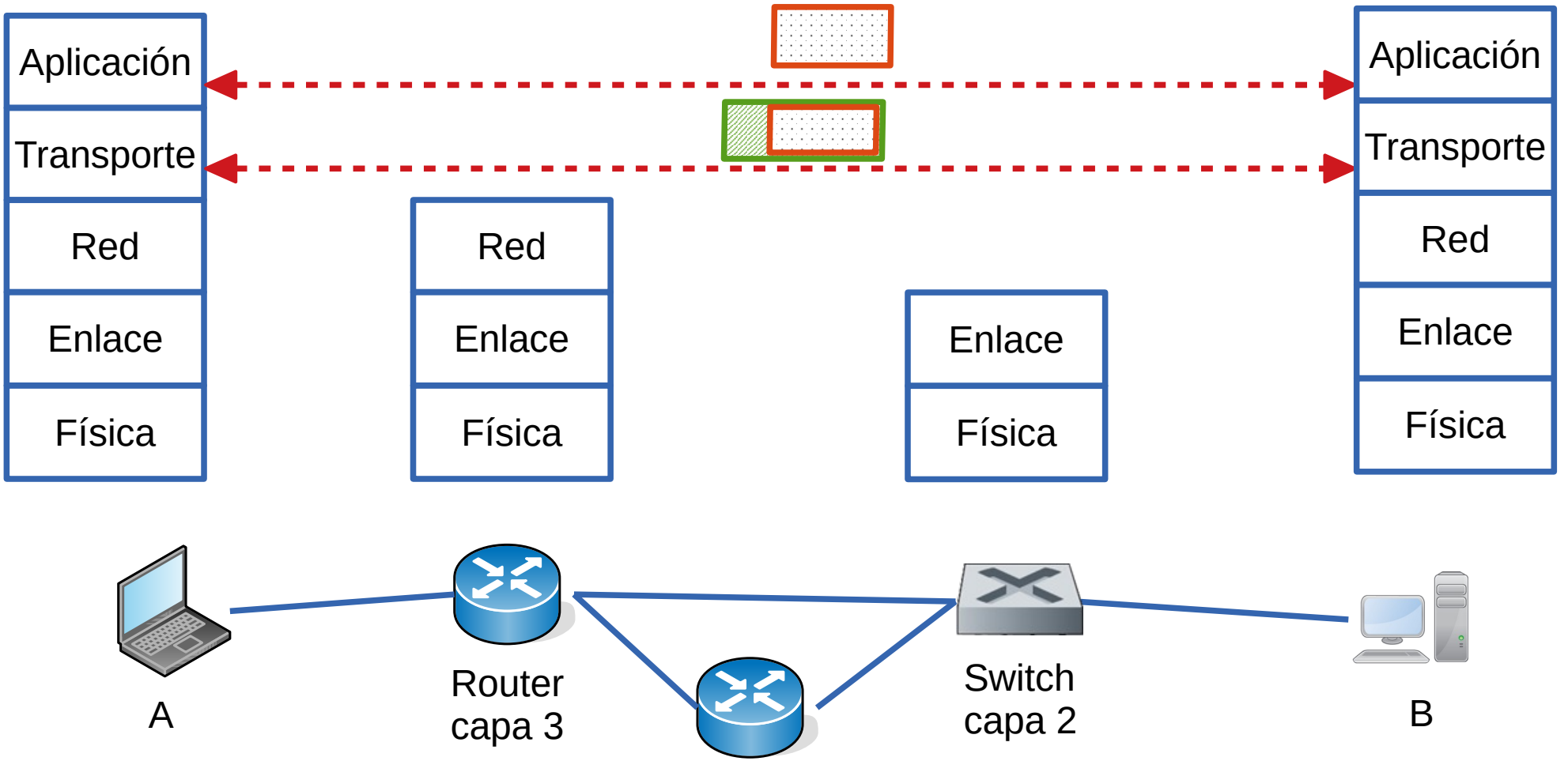
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



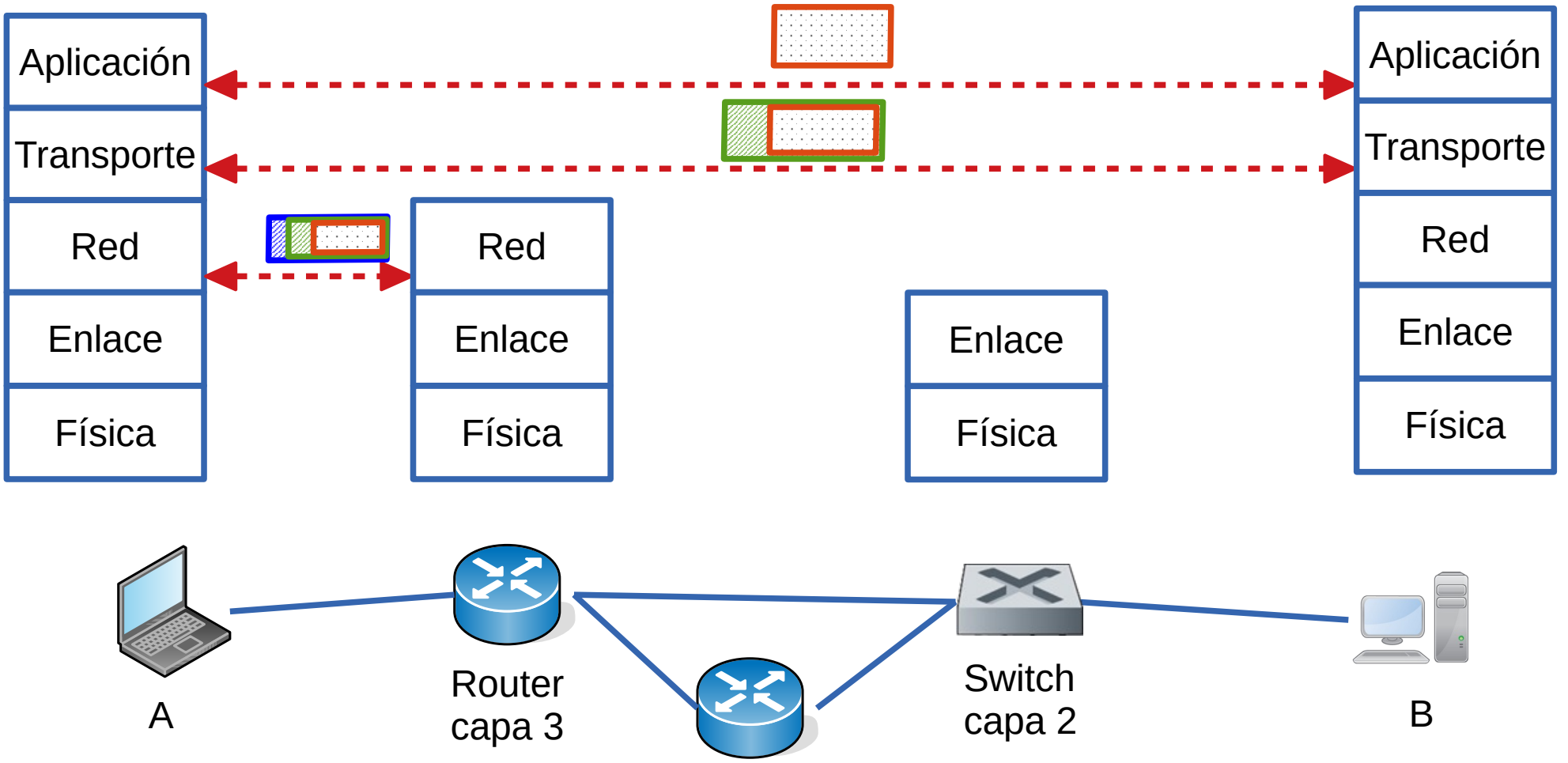
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



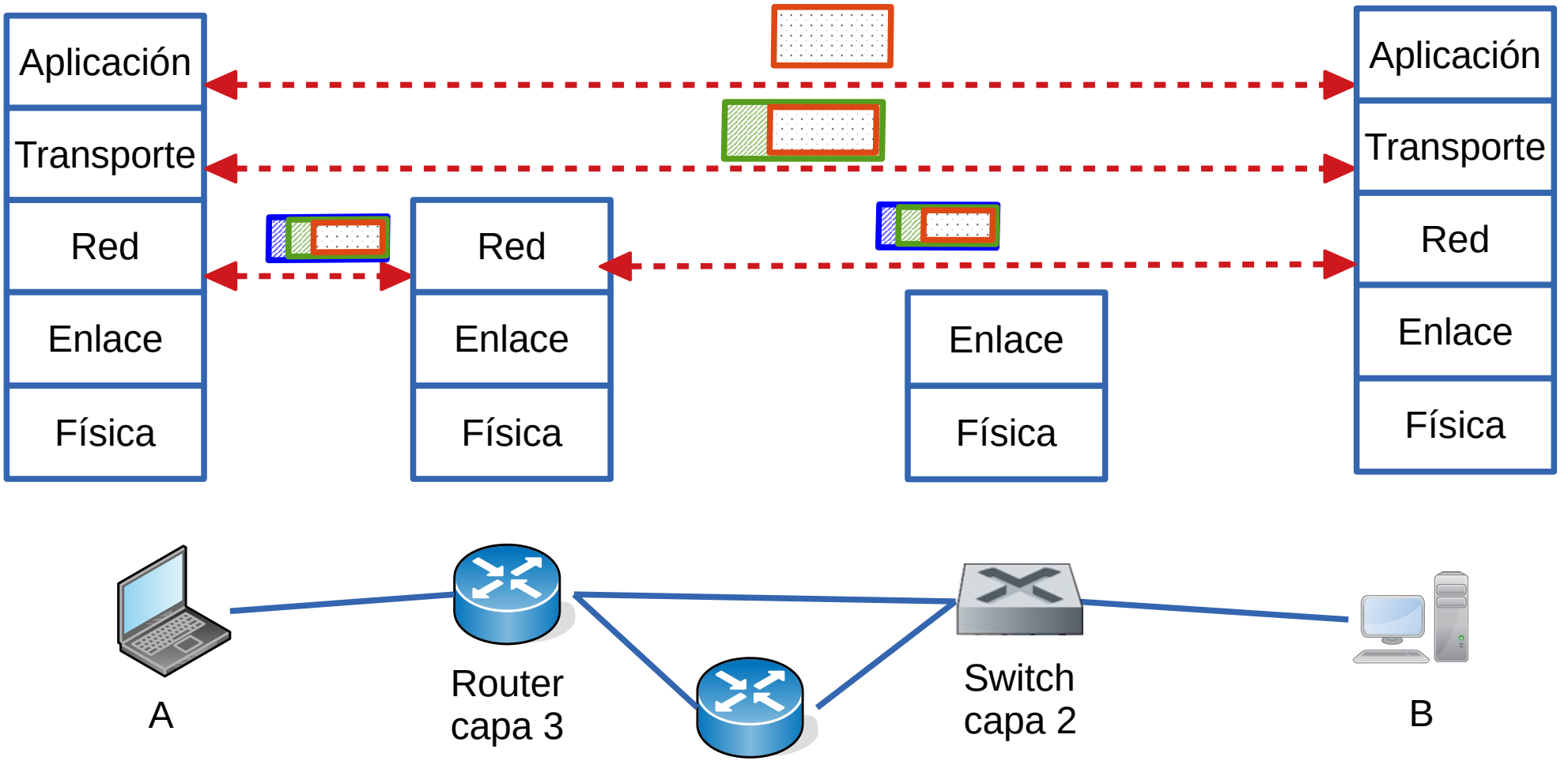
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



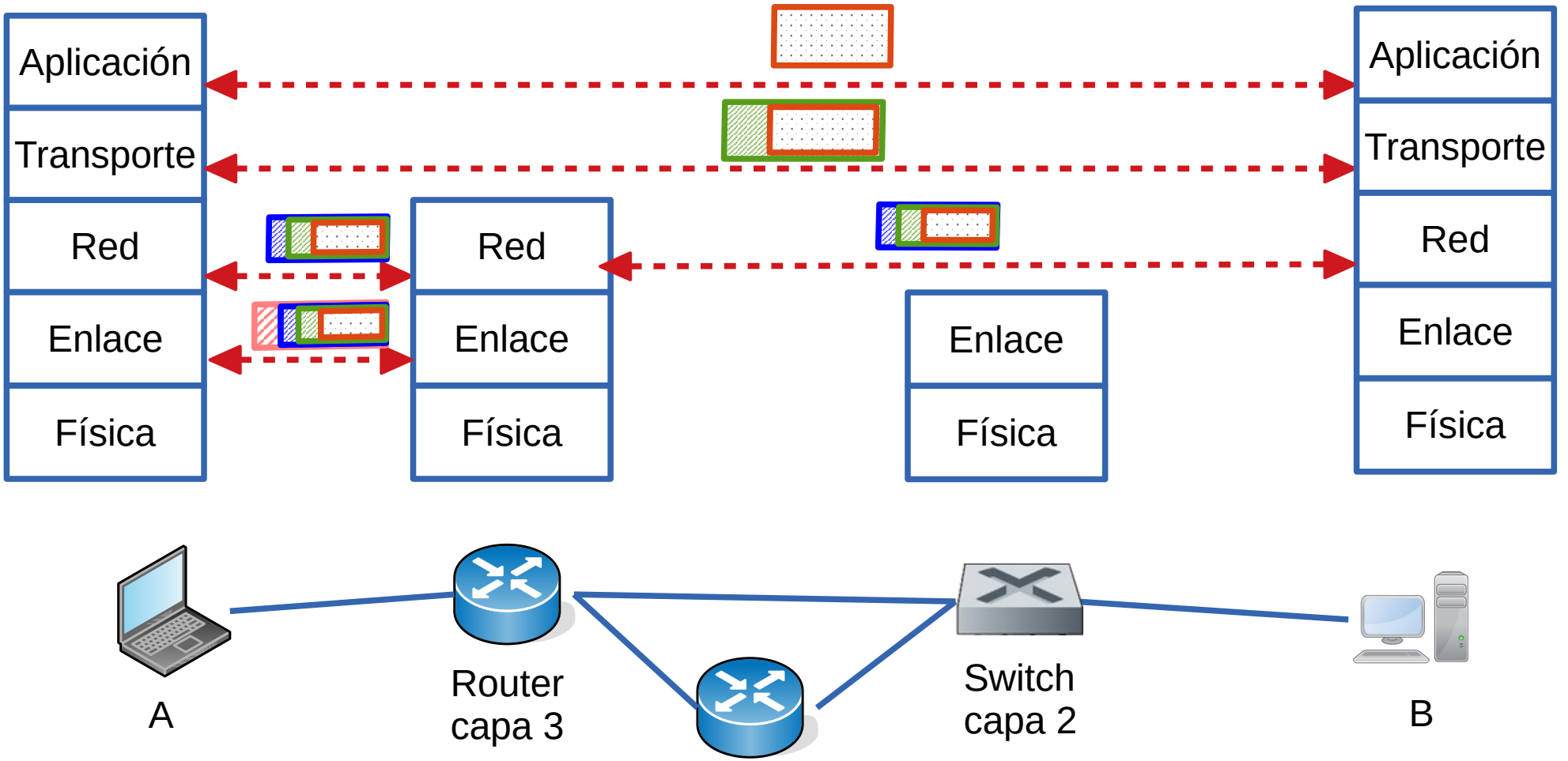
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



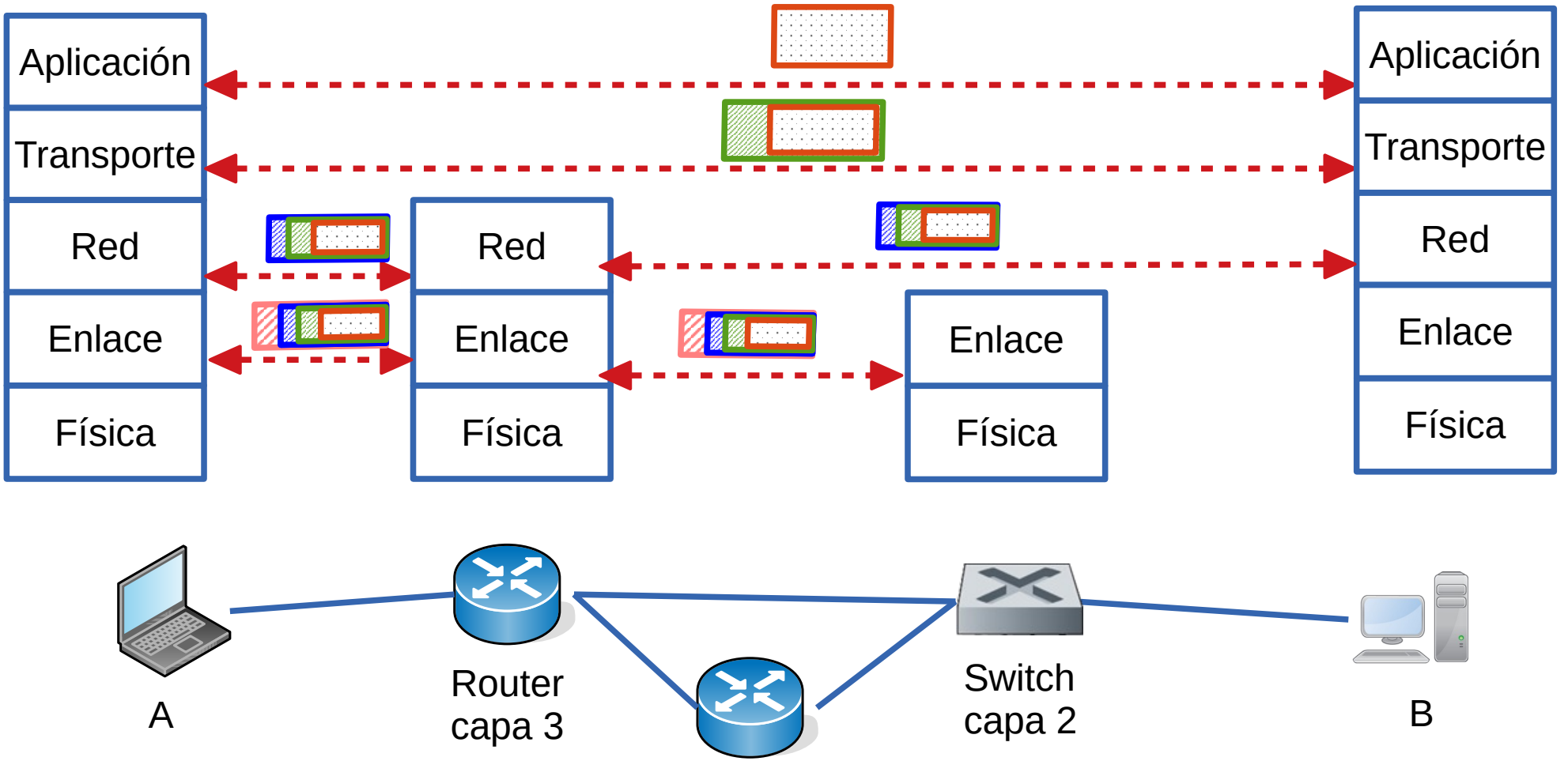
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



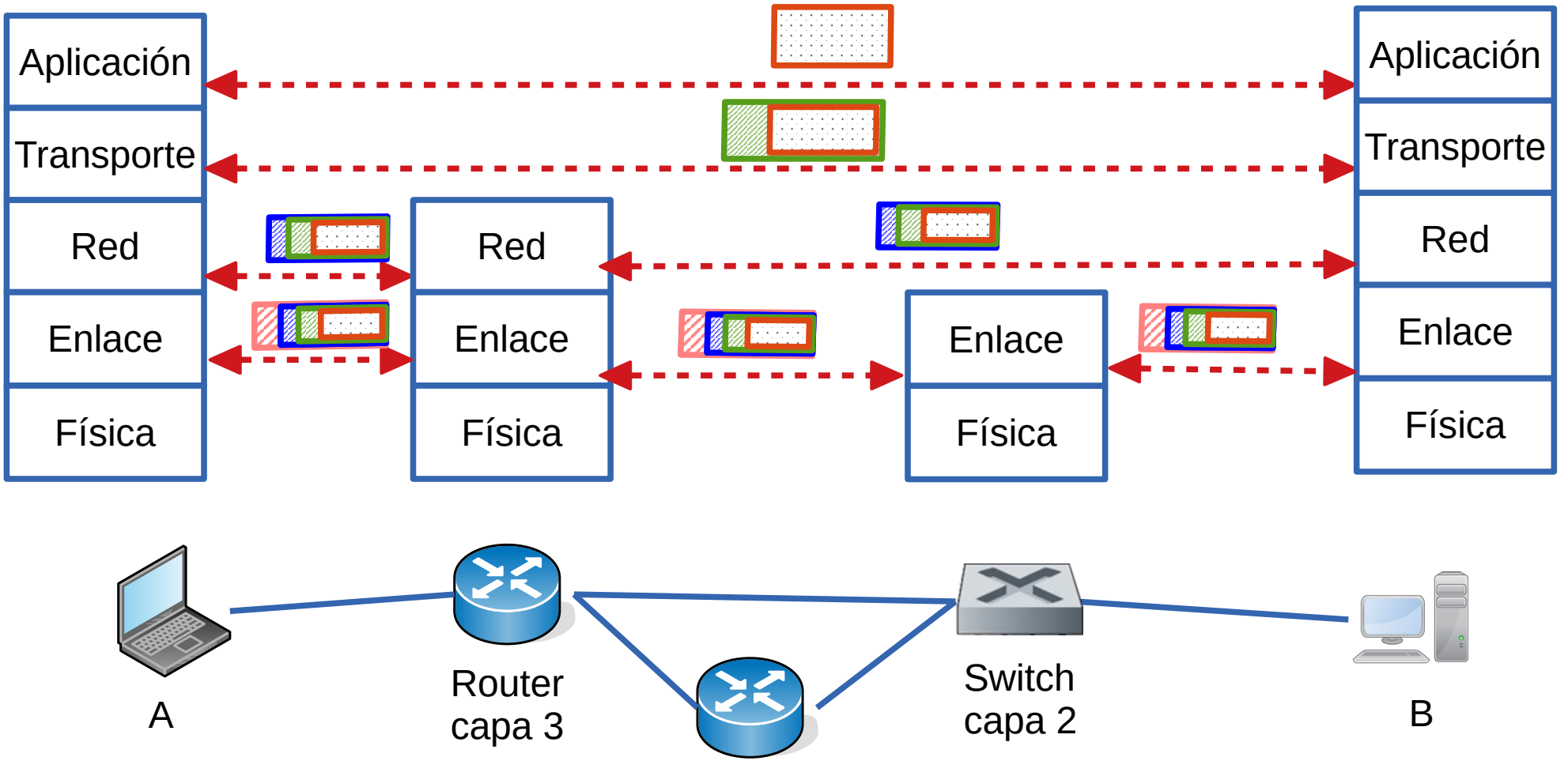
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



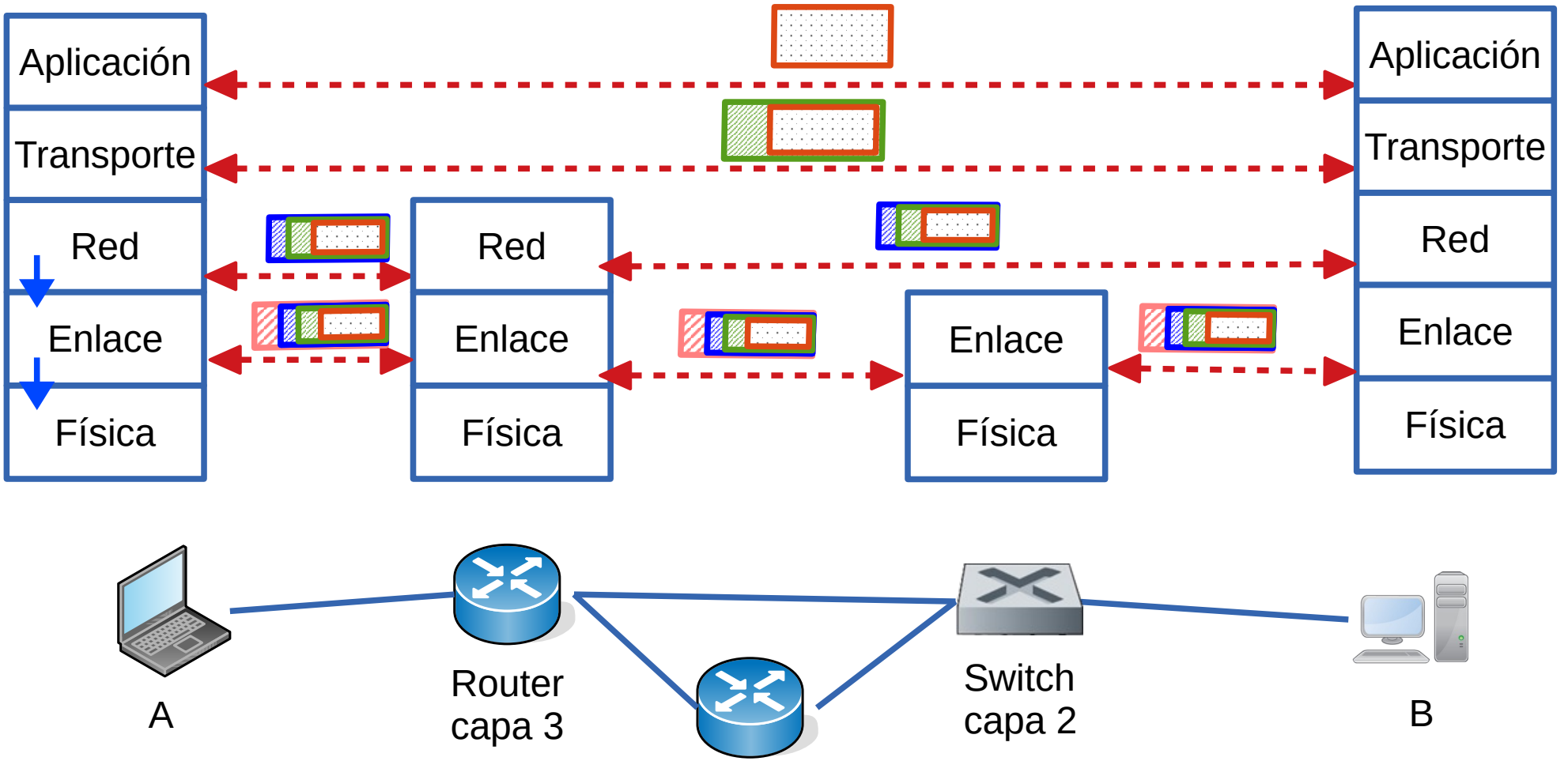
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



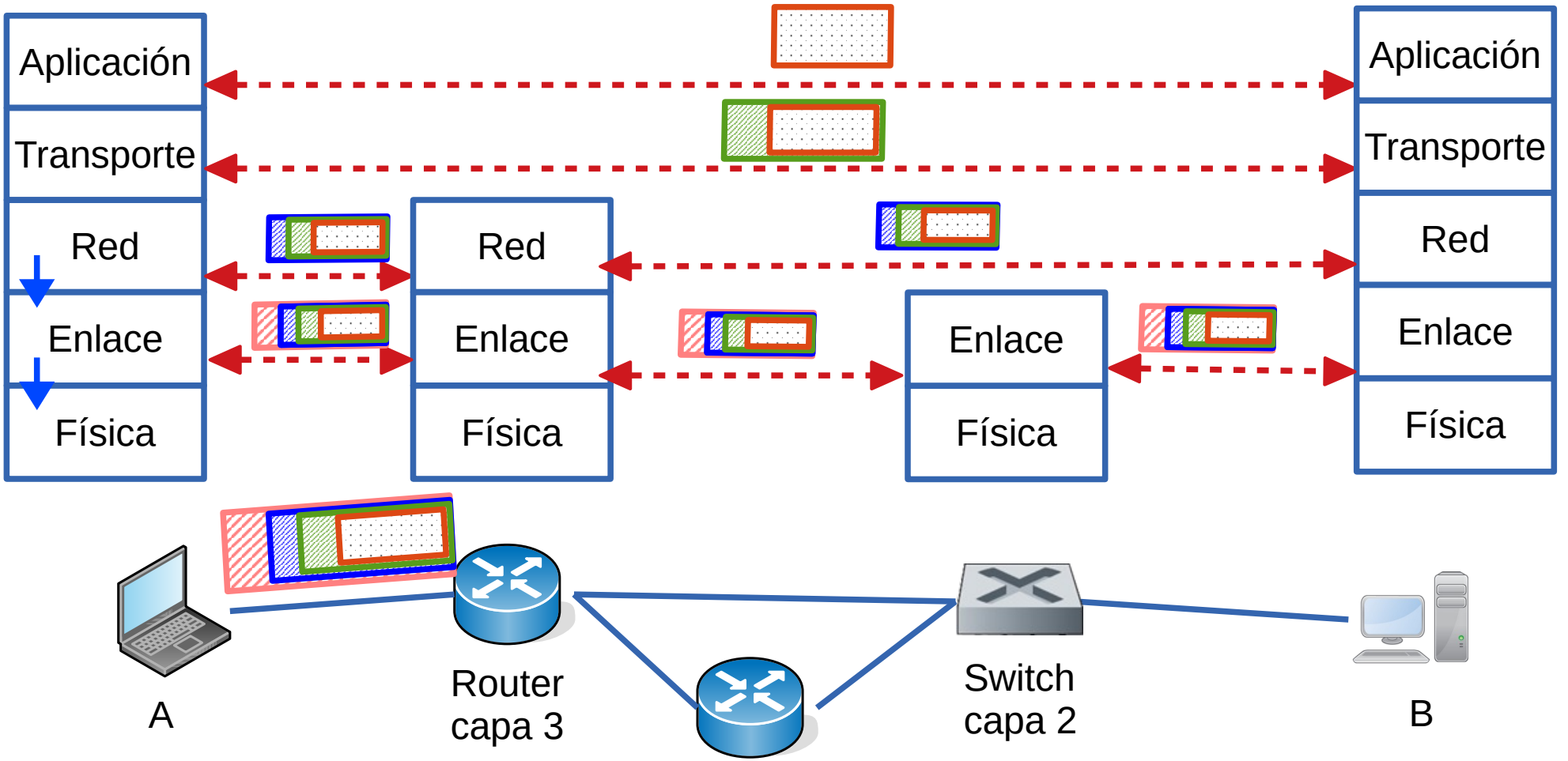
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



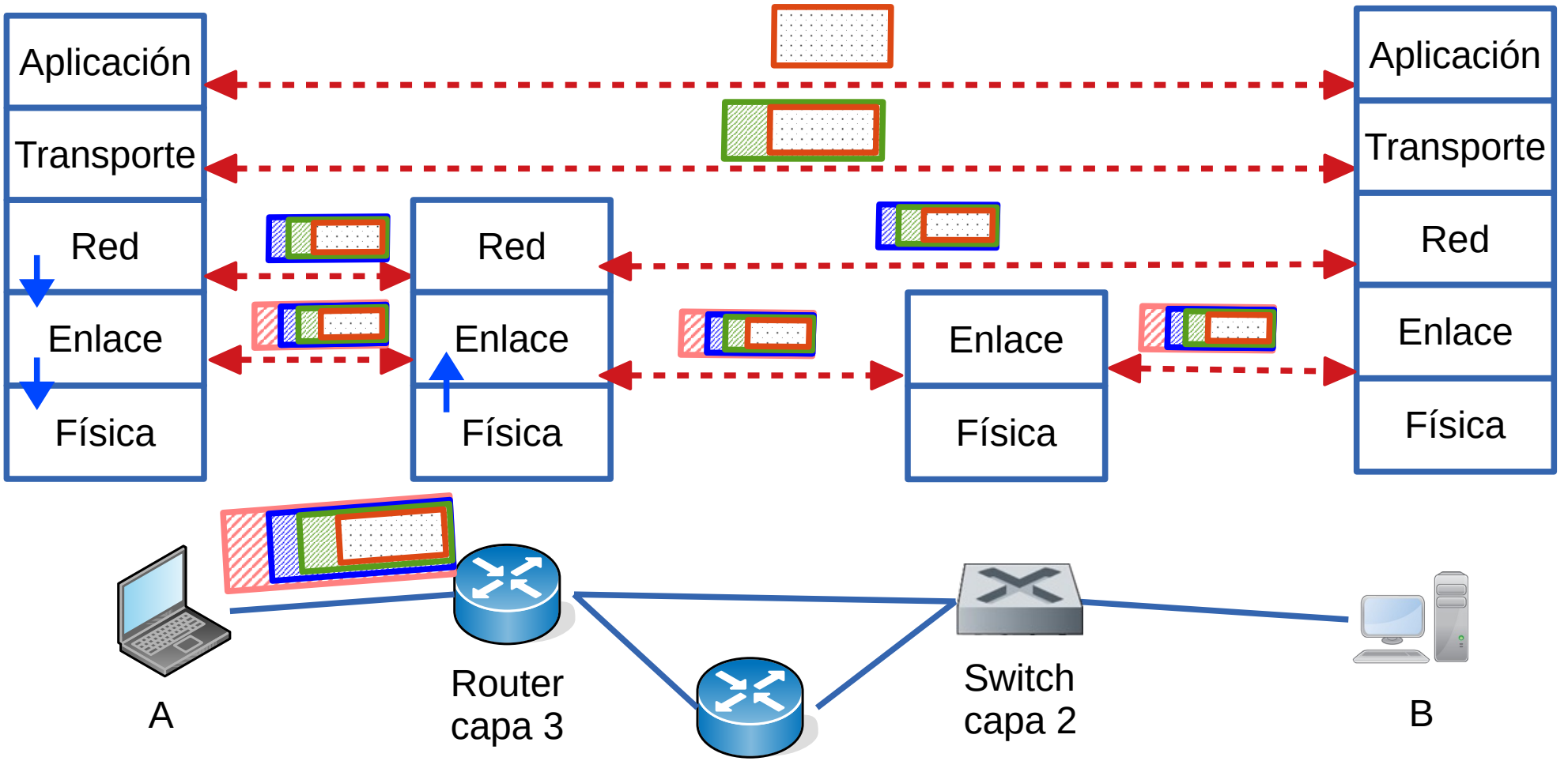
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



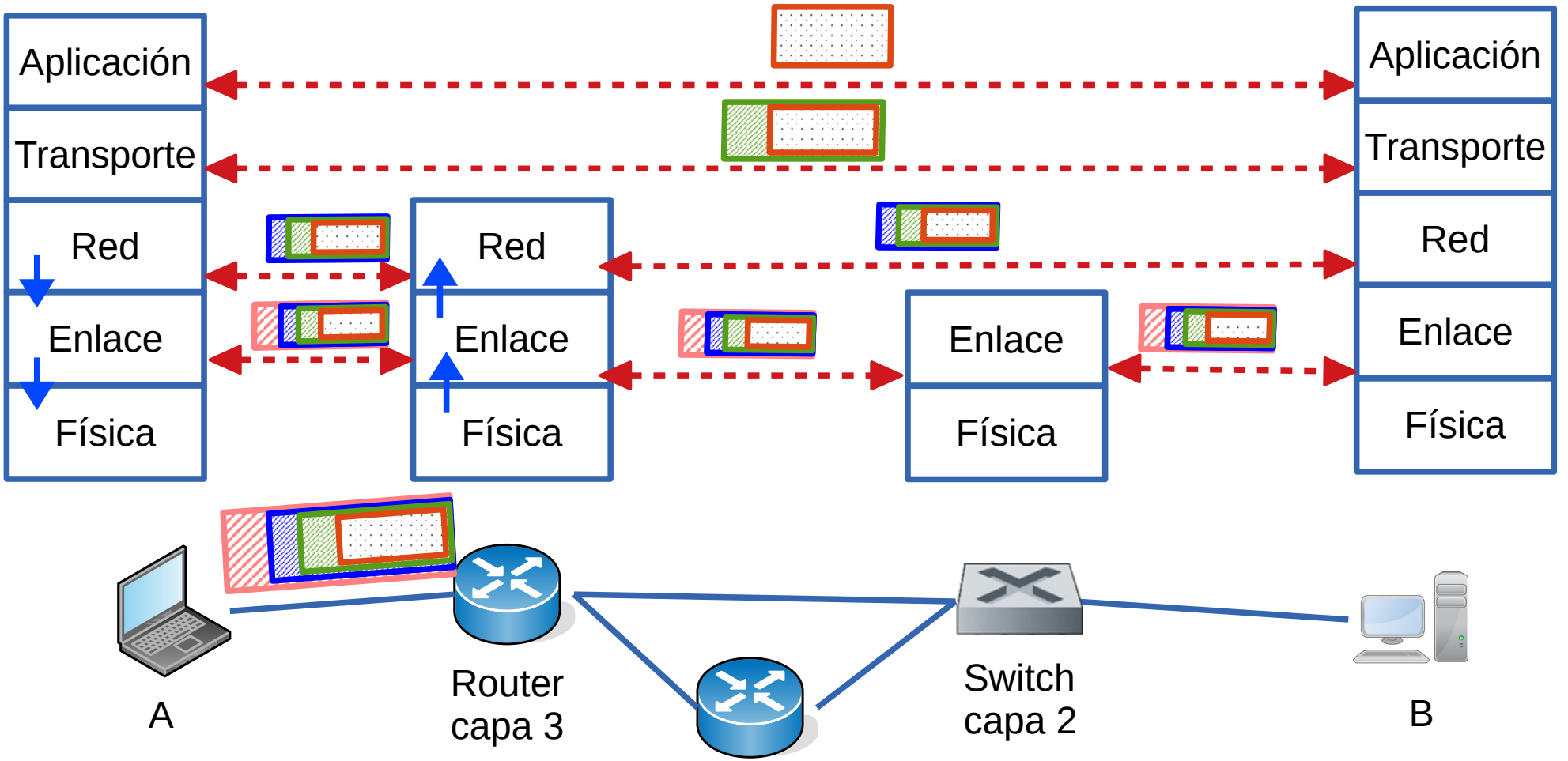
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



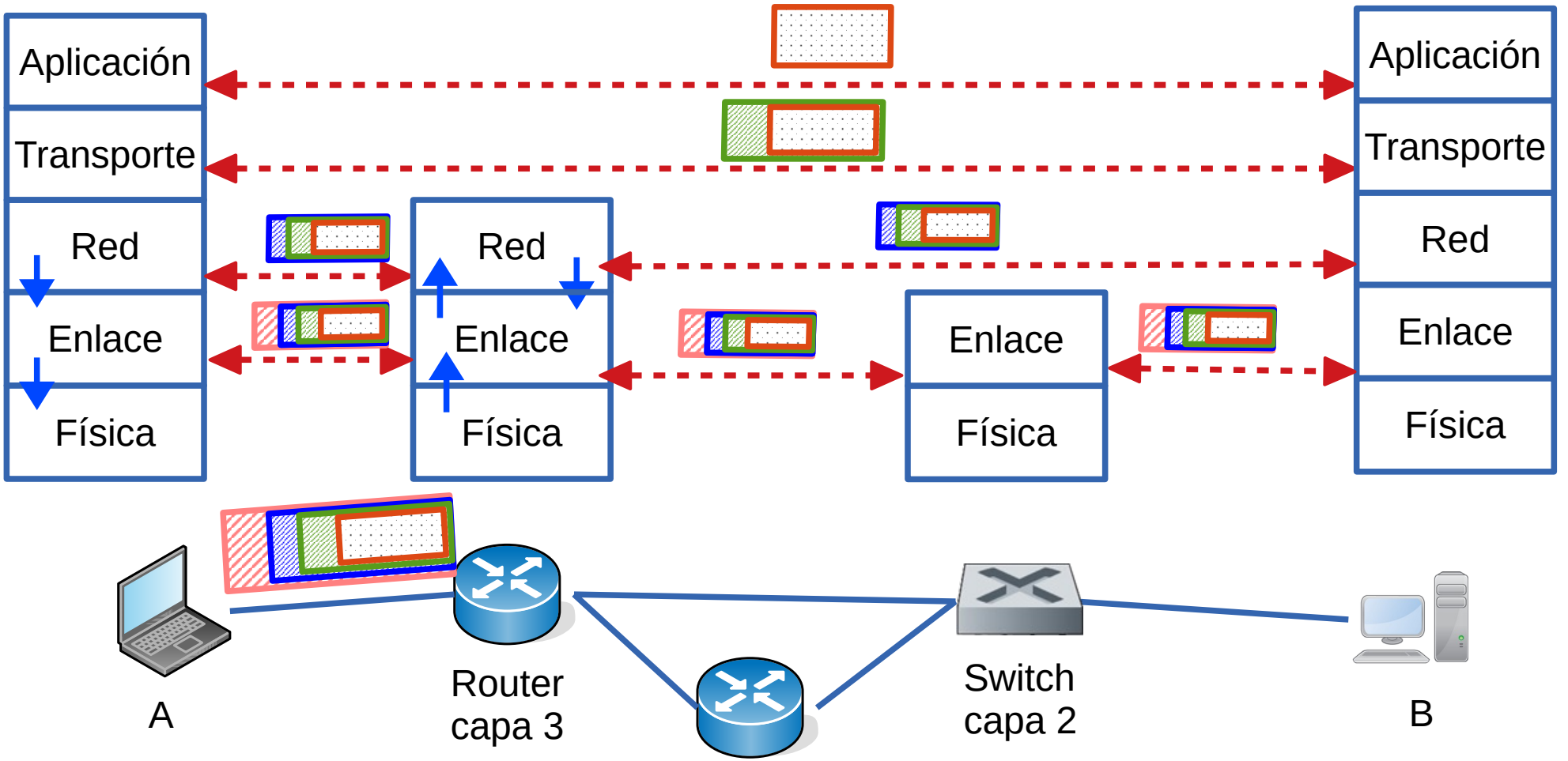
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



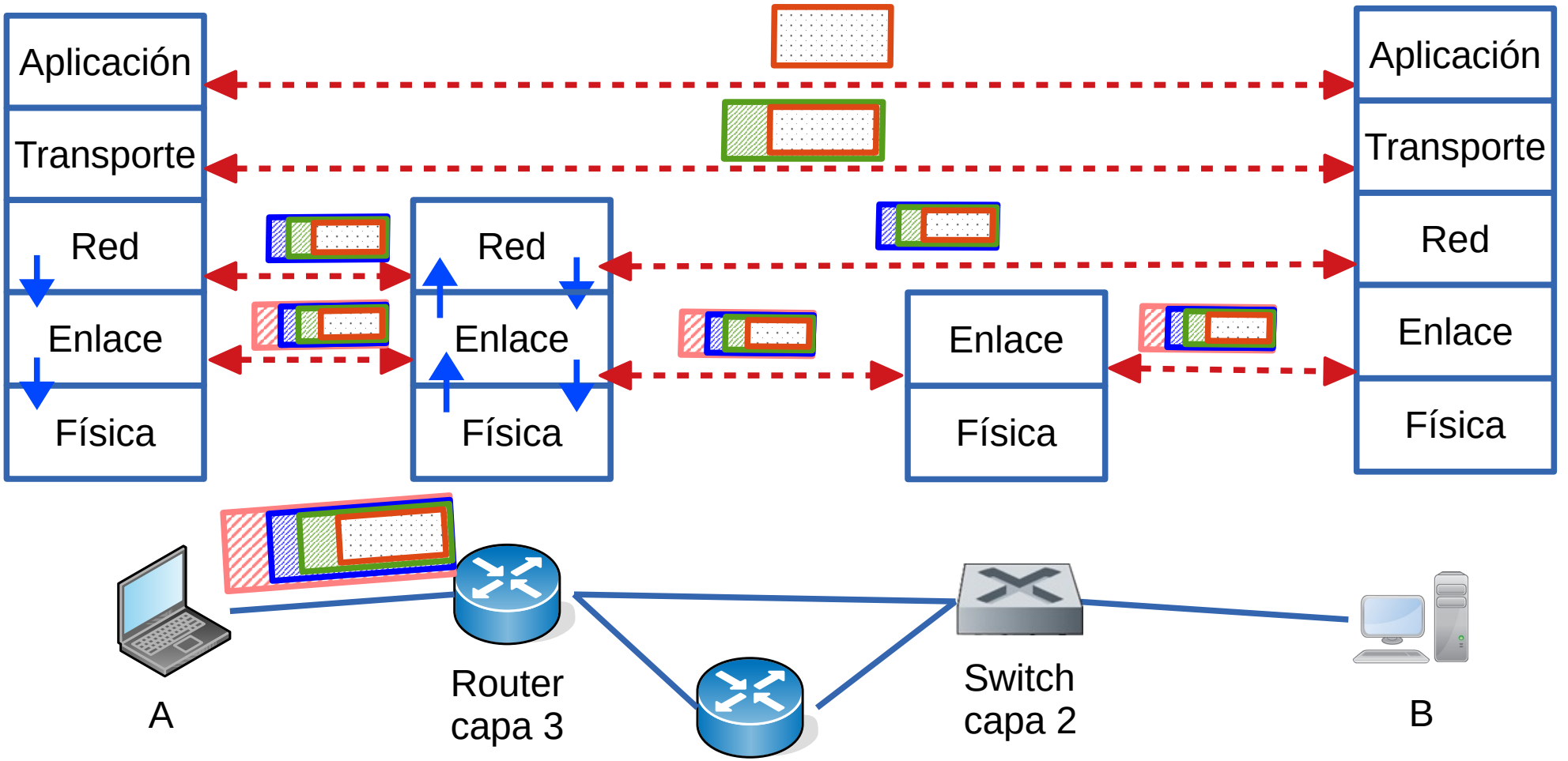
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



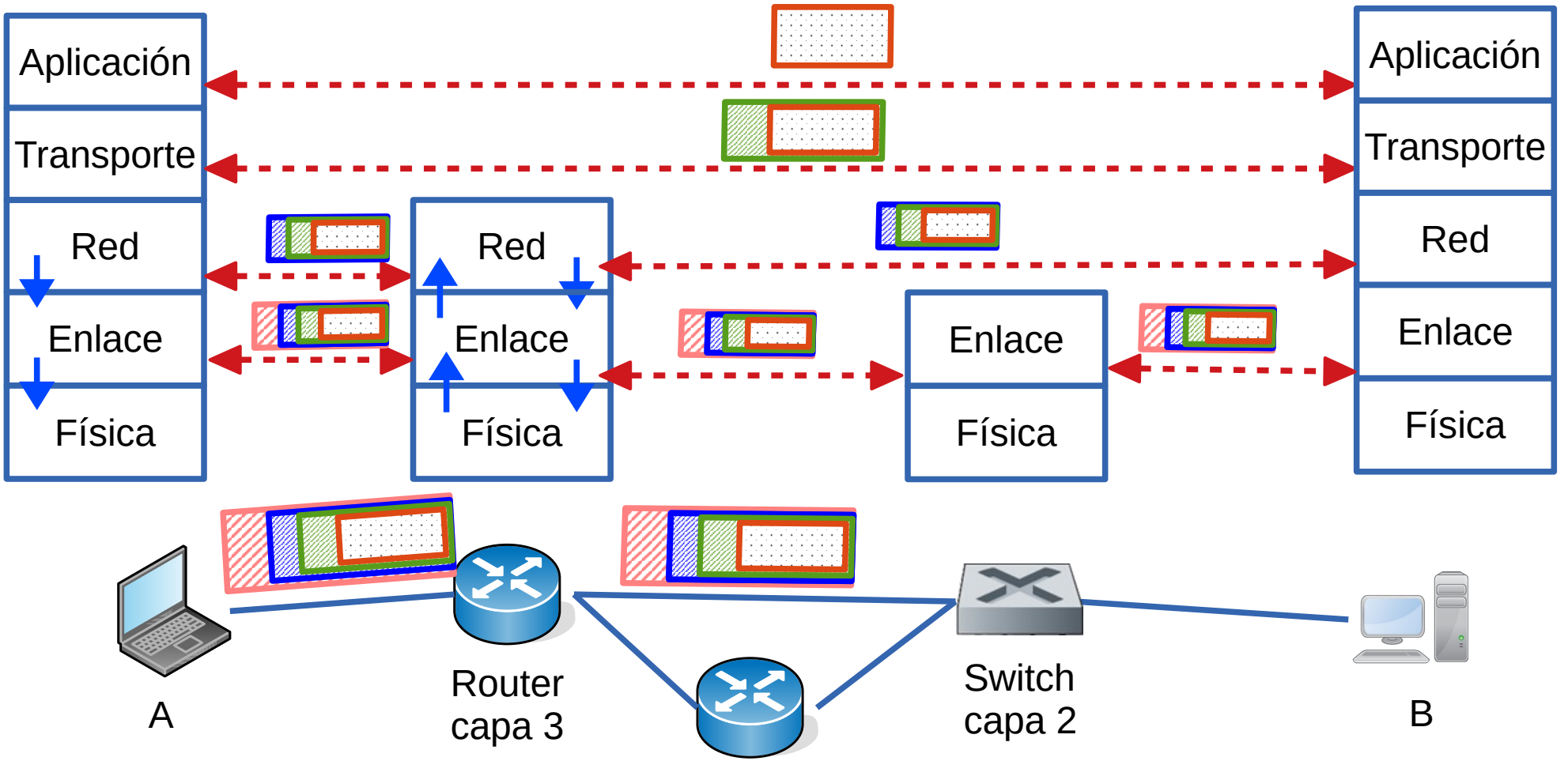
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



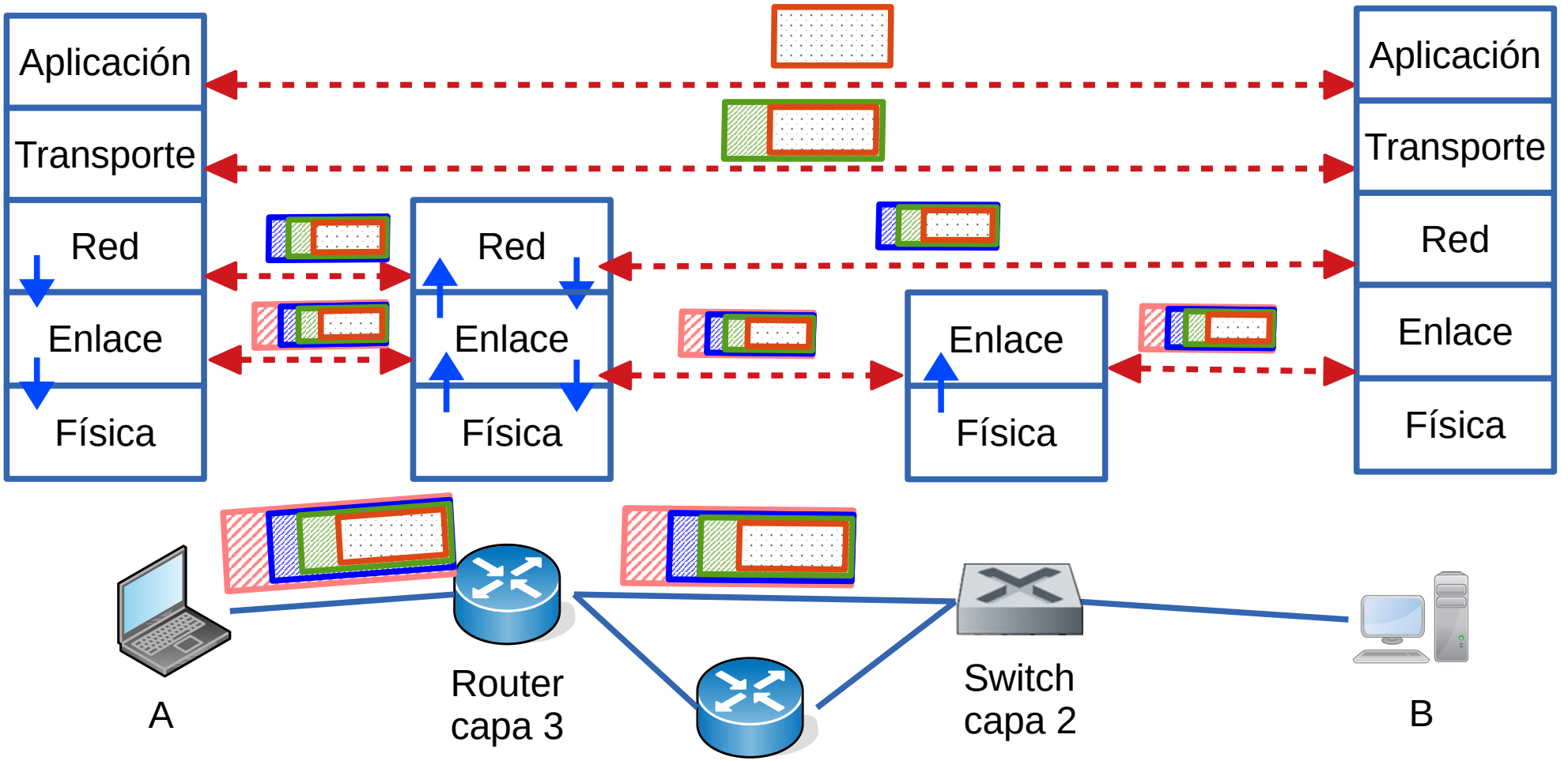
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



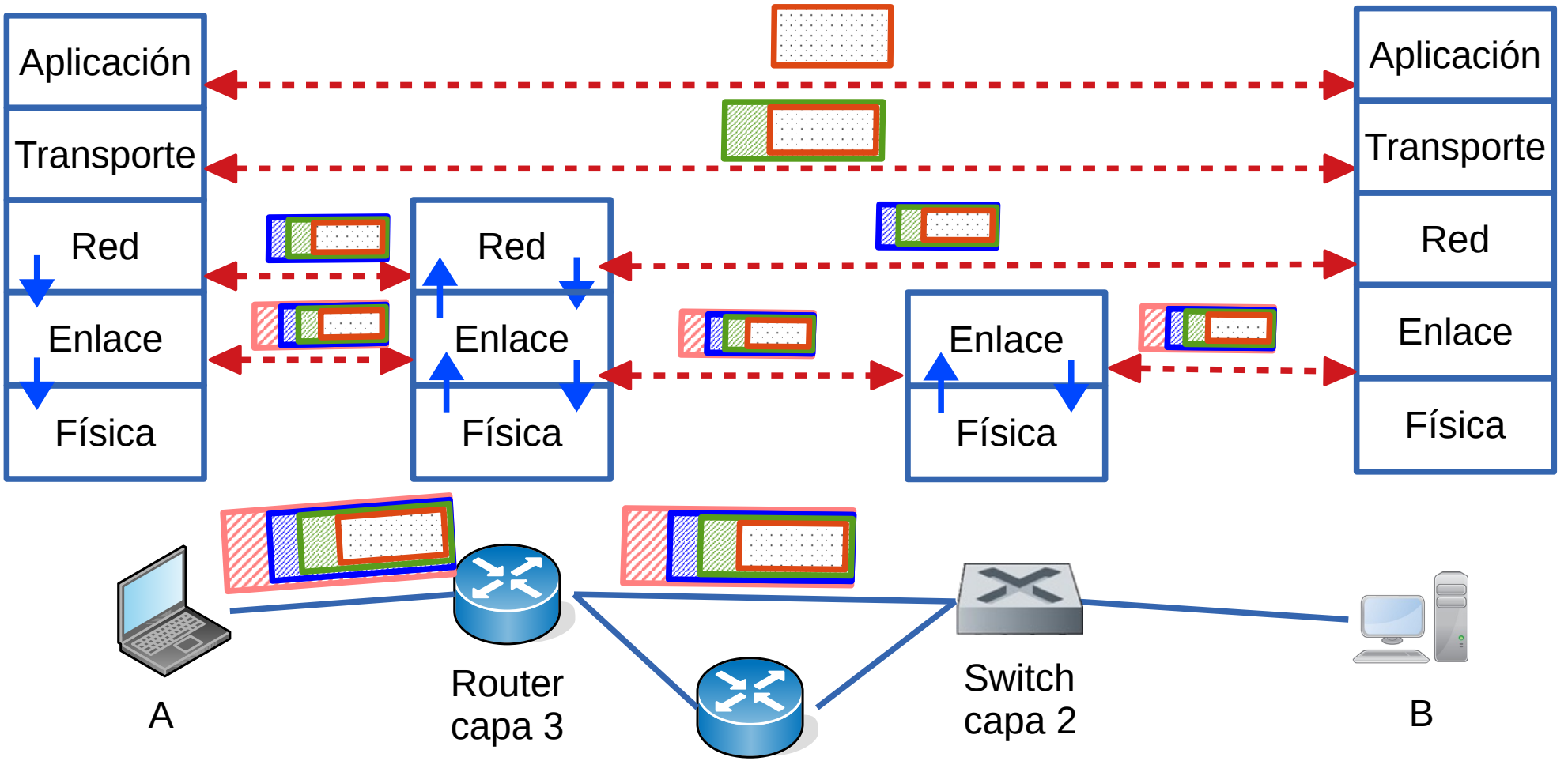
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



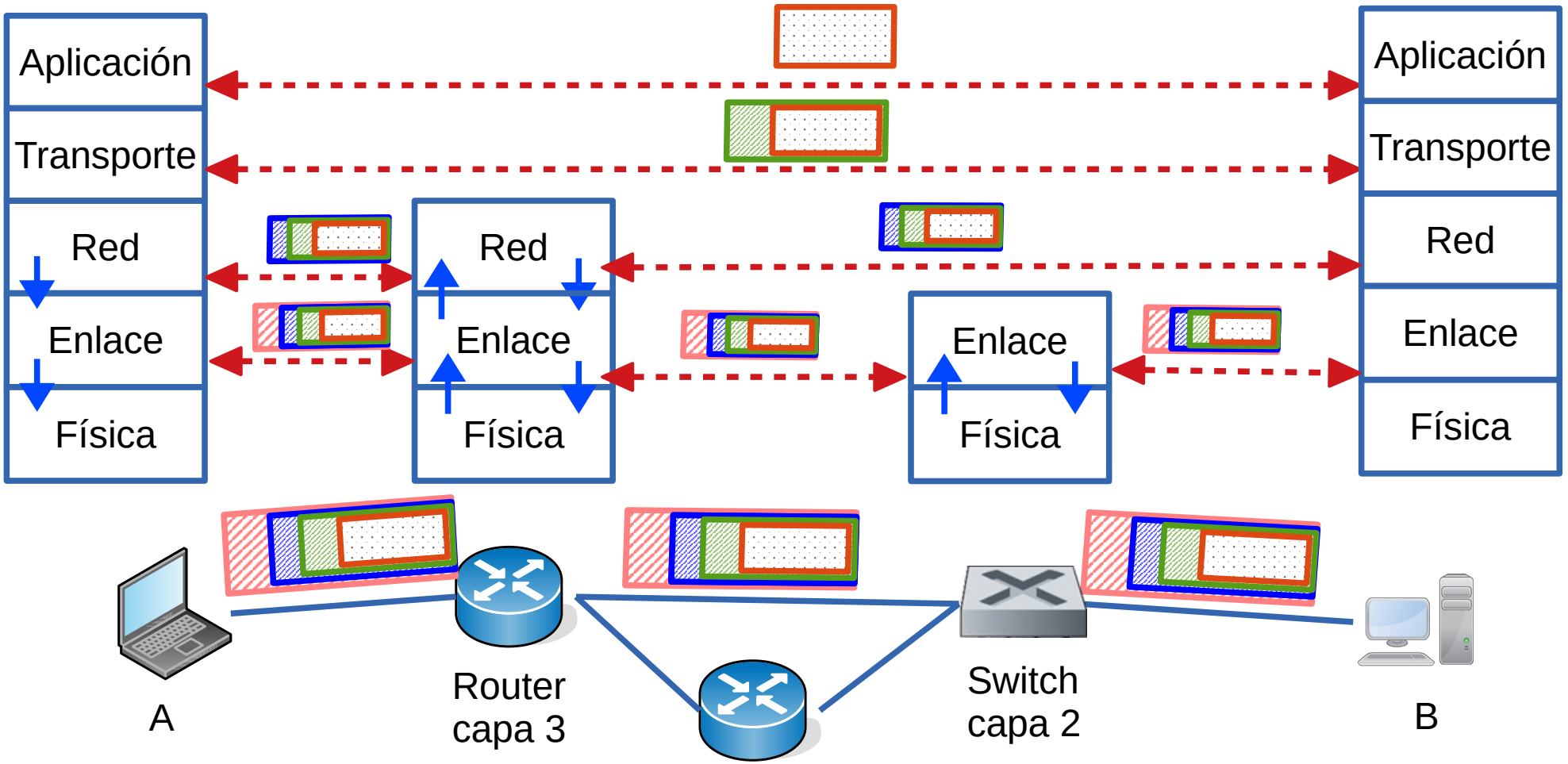
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



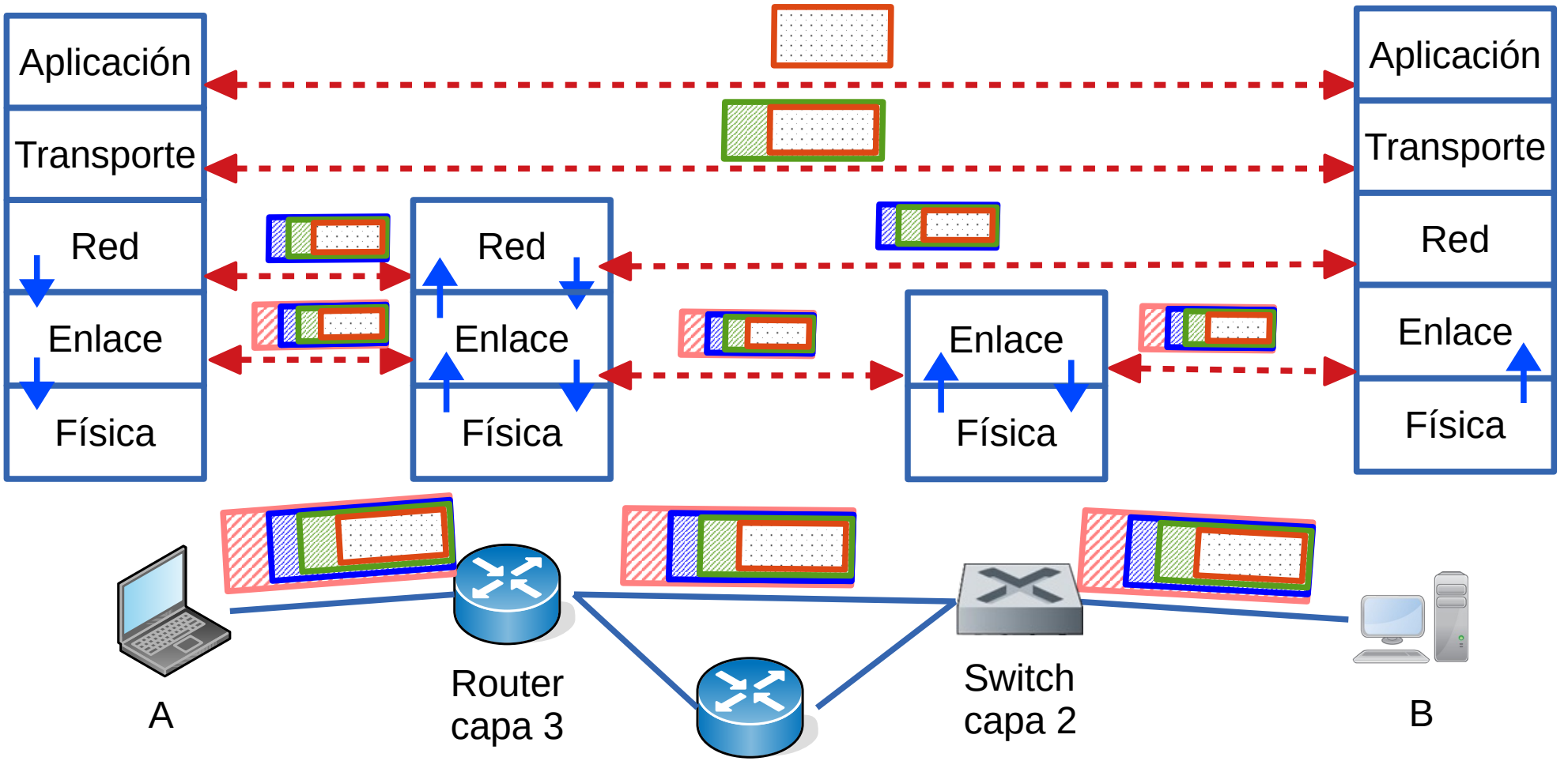
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



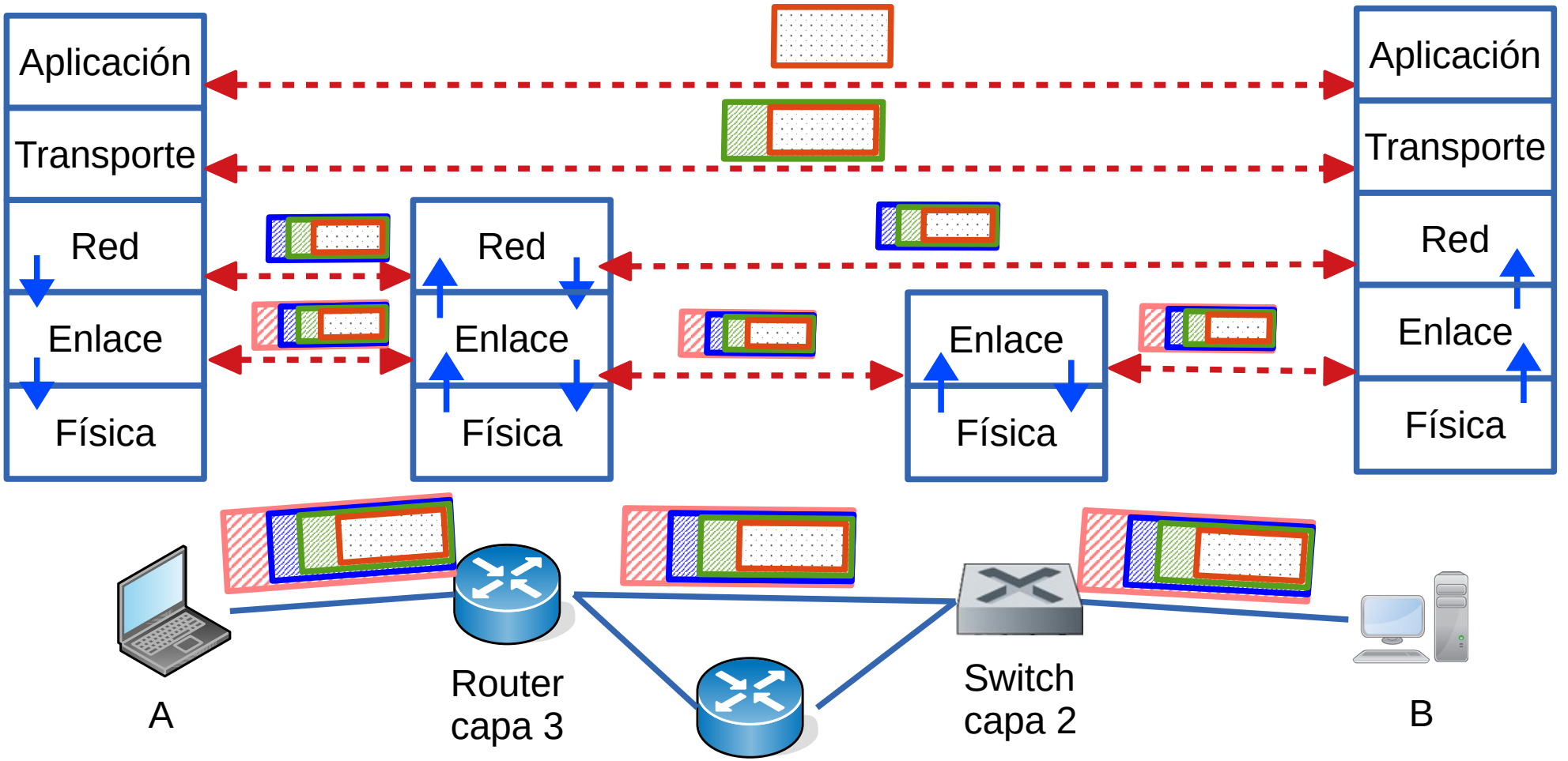
Relación con otras capas

- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



Relación con otras capas

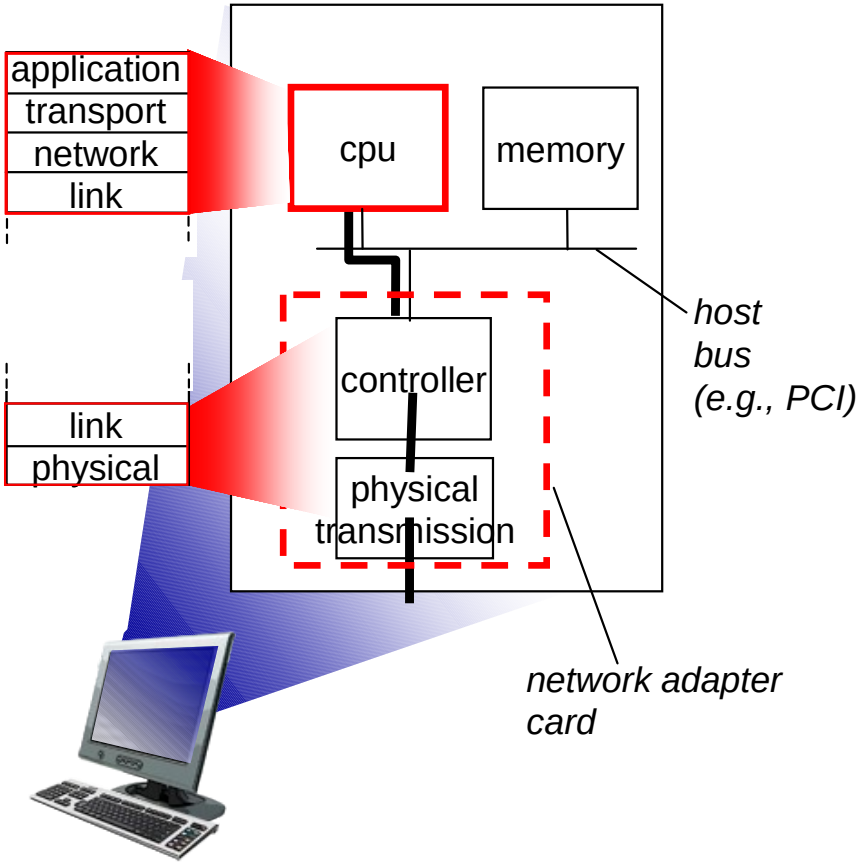
- Brinda servicio a la capa de red
  - Le permite conectarse a través de un link a un nodo adyacente
- Utiliza los servicios de capa física para enviar los bits de la trama



Capa de Enlace

- Se encarga de controlar la comunicación entre dos máquinas “adyacentes”
- Adyacentes significa conectadas mediante un “cable” o algo que actúa como tal
- Los principales problemas son:
  - Errores del medio físico
  - Retardo de los canales
  - Control de acceso al medio físico

¿Dónde está implementada la capa de enlace?



- Varía de protocolo en protocolo
- Es común que varias funciones se implementen en el adaptador
  - Tarjeta independiente o embebido
  - Ejemplos: Ethernet, WiFi

Principales funciones de la capa de enlace

- Entramado
  - Permitir al receptor detectar dónde comienza y termina una trama
- Control de errores
  - Identificar si lo que recibe el receptor es lo enviado. En algunos protocolos también corrección de errores
- Control de flujo
  - Evitar que se sature un receptor lento o muy ocupado
- Control de acceso a un medio compartido
  - Permitir que múltiples equipos compartan un medio de forma ordenada y equitativa
- Direccionamiento
  - En medios compartidos, identificar el destinatario de los mensajes
- Entrega confiable
  - En caso de requerirlo

Enlaces punto a punto vs medios compartidos

- Enlaces punto a punto: exactamente 2 equipos, interconectados mediante algún medio físico
  - Todo lo que envíe será recibido por el otro nodo
  - No preciso direccionamiento ni control de acceso al canal
  - Half duplex (un solo medio) o full duplex (un canal de ida y uno de vuelta)
  - Ejemplo: enlace directo entre 2 equipos
- Medios compartidos: múltiples equipos pueden acceder al mismo medio
  - Ejemplo: red de área local inalámbrica (WiFi)
  - Se requiere direccionamiento para elegir el destino
  - Se requieren protocolos para ordenar el acceso al medio compartido
  - Surge una sub-capa: MAC (Medium Access Control)

Entramado (framing)

- La capa 2 para dar el servicio a la capa de red debe valerse de la capa física
- Como hay errores en la capa física hay que detectar y eventualmente corregir errores
- Idea principal: división en tramas y hacer un control de error en cada trama
- La división en tramas no es tan sencilla
- Múltiples métodos de entramado
  - Conteo de caracteres
  - Caracteres de delimitación
  - Banderas de delimitación
  - Violaciones del código de línea de la capa física
  - Otros
- La capa de enlace le agrega a la información de capa de red un encabezado y posiblemente un trailer (bits al final del mensaje), y le aplica algún método de entramado

Conteo de caracteres

- Se indica el largo de cada trama
- Para saber dónde comienza la siguiente trama, se cuentan los caracteres

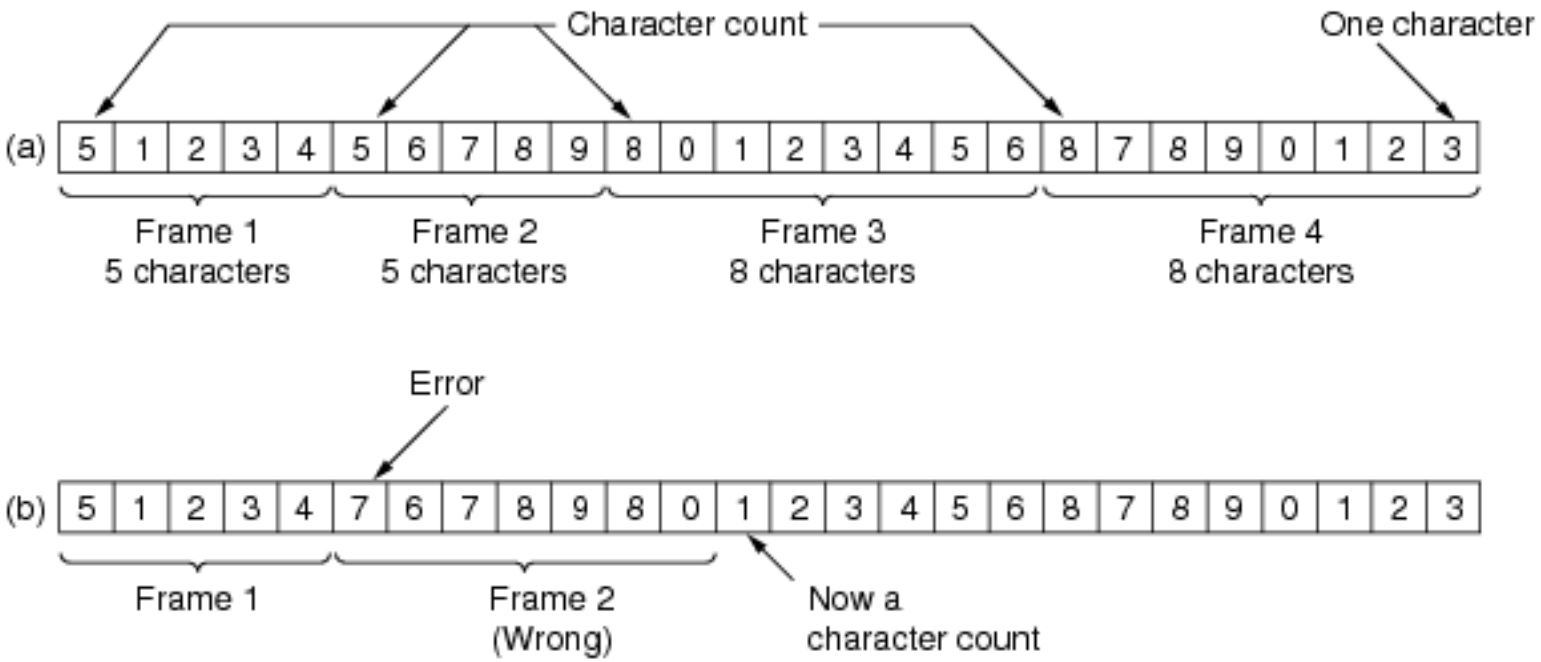


Fig. 3-4. A character stream. (a) Without errors. (b) With one error.

Conteo de caracteres (cont.)

- Problema: ¿qué pasa si se recibe con error el campo de “largo” de la trama?
  - Si se corrompe el encabezado de la trama se pierden las fronteras de tramas
  - Difícil re-sincronizar

Caracteres de principio y fin

- Pensado en la época en que se transmitía mayoritariamente texto ASCII
- Insertar banderas para delimitar el comienzo y fin de la trama
- Comúnmente se delimita con caracteres ASCII especiales (de control)
  - DLE STX = bandera de comienzo
  - DLE ETX = bandera de fin
- Se transmite:

- El receptor detecta el principio y fin de trama buscando esa secuencia de caracteres
- ¿Qué pasa si aparece DLE STX (o DLE ETX) entre los datos de capa de red?

Inserción de caracteres para lograr transparencia

- Recibido de la capa de red en el Tx:

- Inserción de caracteres:

- Inserción de banderas (lo que se transmite):

- En el receptor se procesa de modo que:
  - DLE STX = bandera de comienzo
  - DLE DLE = se saca un DLE
  - DLE ETX = bandera de fin
- Se entrega a la capa de red en el Rx:

Inserción de caracteres. Problemas

- Muy atado a transmisión de caracteres de 8 bits
- Optimizado para contenido ASCII

Banderas e inserción de bits

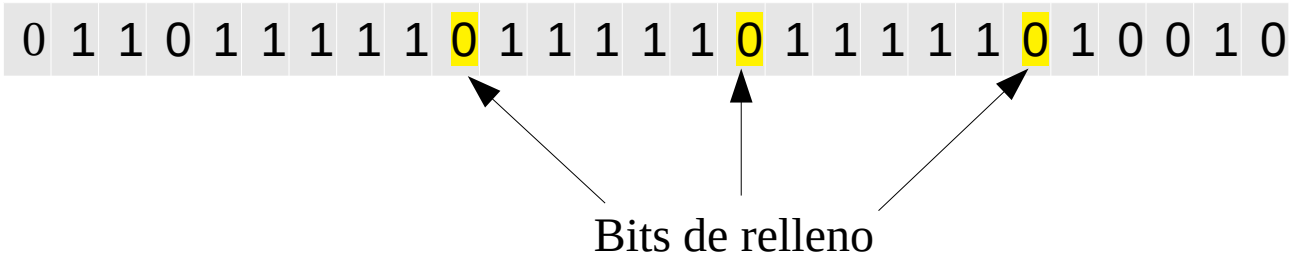
- Misma idea que inserción de caracteres pero con banderas definidas como patrones de bits
- Bandera típica 01111110 = 7E hexadecimal
- Se debe evitar que la bandera aparezca en los datos
- Si la bandera se da en los datos, se insertan bits de relleno
- En transmisión:
  - Se interrumpe cualquier secuencia de 6 “1”s seguidos insertando un “0” luego del quinto “1”
  - Sin importar lo que venga después!!!
  - Se insertan las banderas y se envía al receptor
- En recepción:
  - Se reconocen las banderas 01111110
  - Si se ven 5 “1” y un “0” se saca el “0”
  - Sin importar lo que venga después!!!

Banderas e inserción de bits

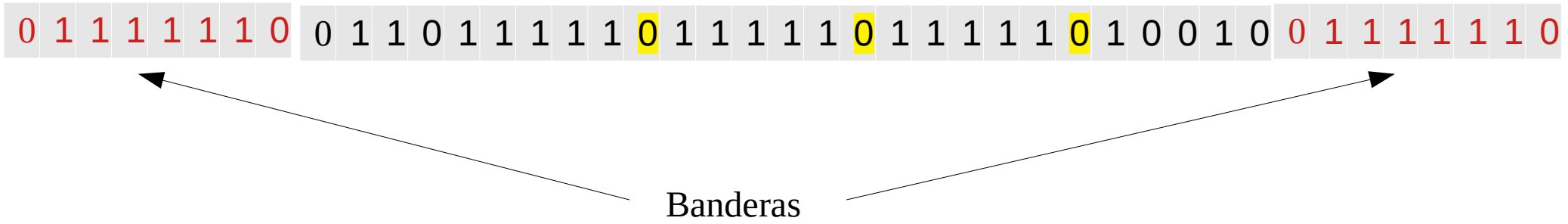
- Datos de capa 3 a transmiitir

0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

- Inserción de bits para lograr transparencia



- Bits a transmitir por el canal de comunicaciones luego de agregar las banderas

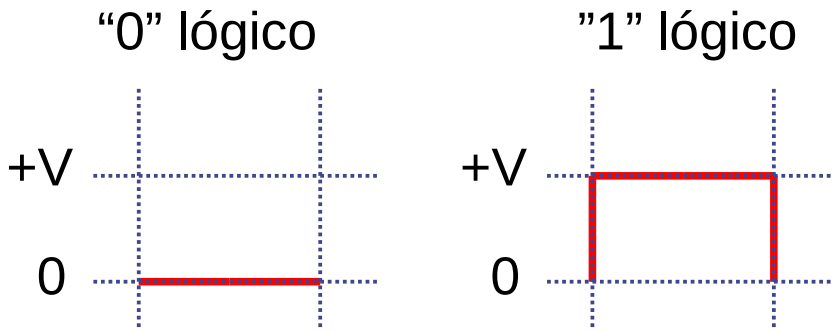


Violaciones del código de línea

- En capa física se utilizan símbolos (típicamente combinaciones de amplitud/frecuencia/fase u otras magnitudes) para representar uno o más bits
- Podemos reservar algún símbolo de capa física para representar el inicio y/o fin de trama
- También podemos utilizar alguna combinación inválida de magnitudes con esta misma función
- Problema: viola la independencia de capas

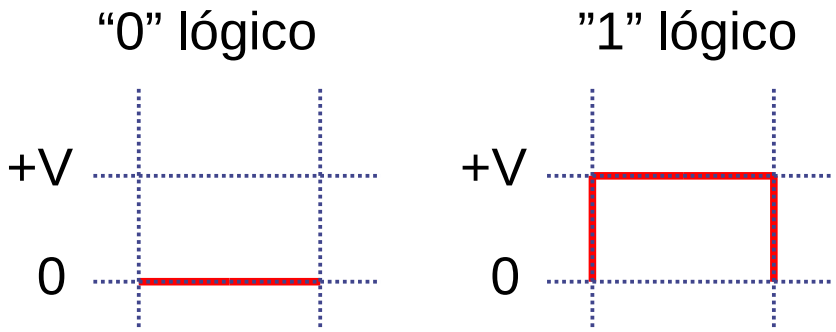
Violaciones del código de línea

- Ejemplo:



Violaciones del código de línea

- Ejemplo:

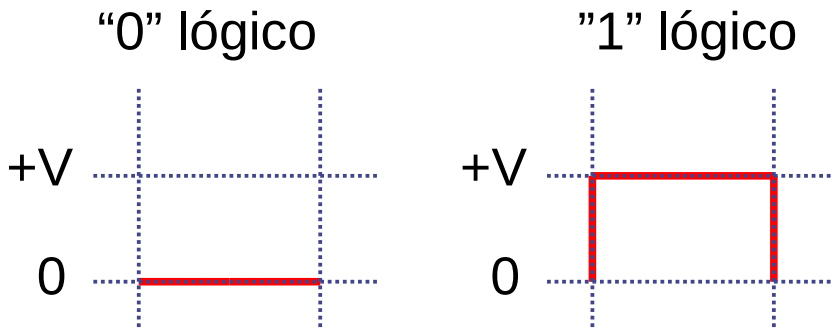


- Secuencias de muchos “1” o muchos “0” seguidos

0 1 1 1 1 1 1

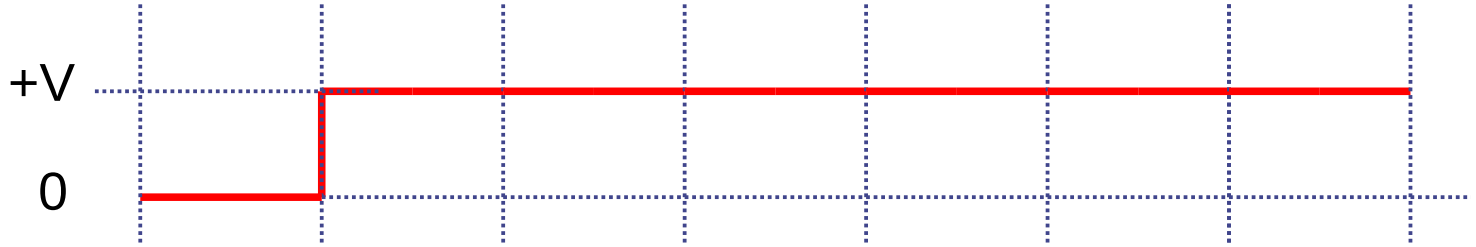
Violaciones del código de línea

- Ejemplo:



- Secuencias de muchos “1” o muchos “0” seguidos

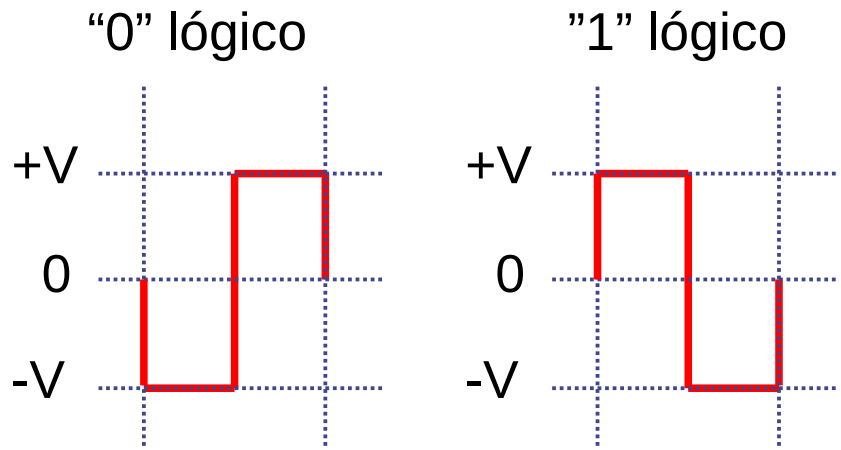
0 1 1 1 1 1 1



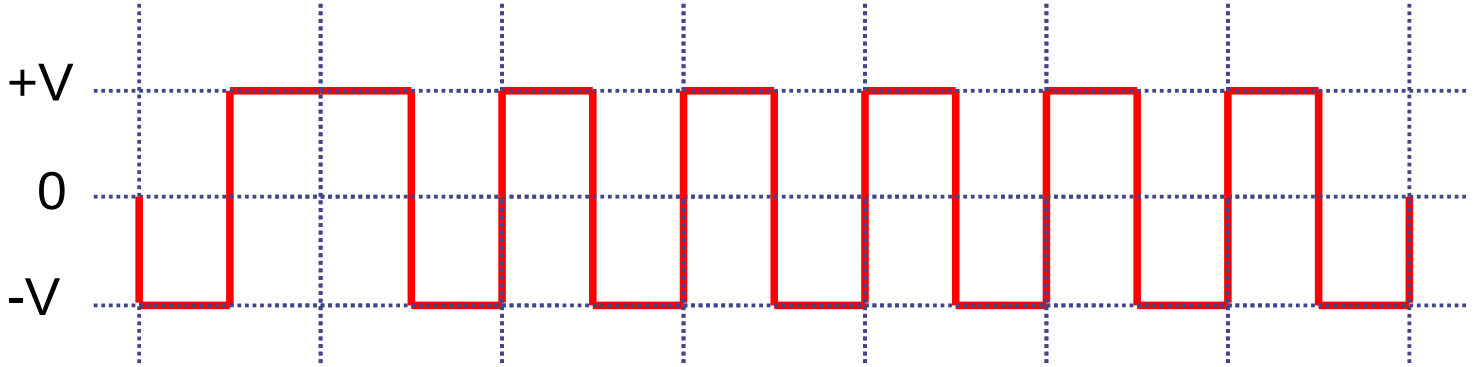
- Generan señales:
  - que no tienen nivel de continua 0
  - en las que no se puede recuperar el reloj (las fronteras de bits)

Violaciones del código de línea

- Pero si uso por ejemplo:



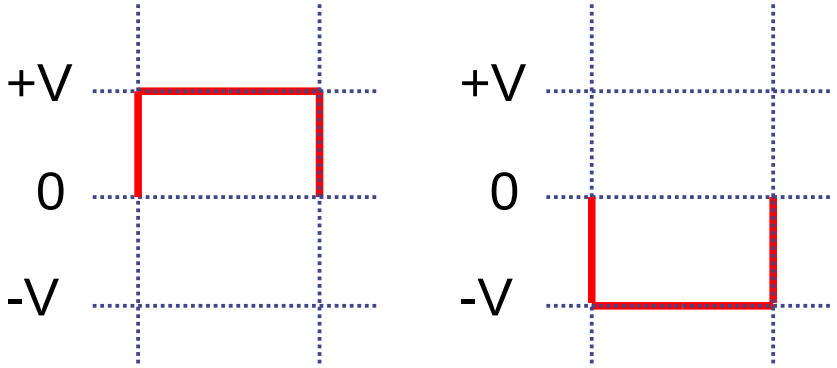
- La misma secuencia queda: 0 1 1 1 1 1 1



- Que tiene nivel de continua 0 y flancos de reloj que permiten sincronizarse

Violaciones del código de línea

- Pero aparecen dos combinaciones que no representan ni un “0” ni un “1” y podrían usarse para delimitar tramas:

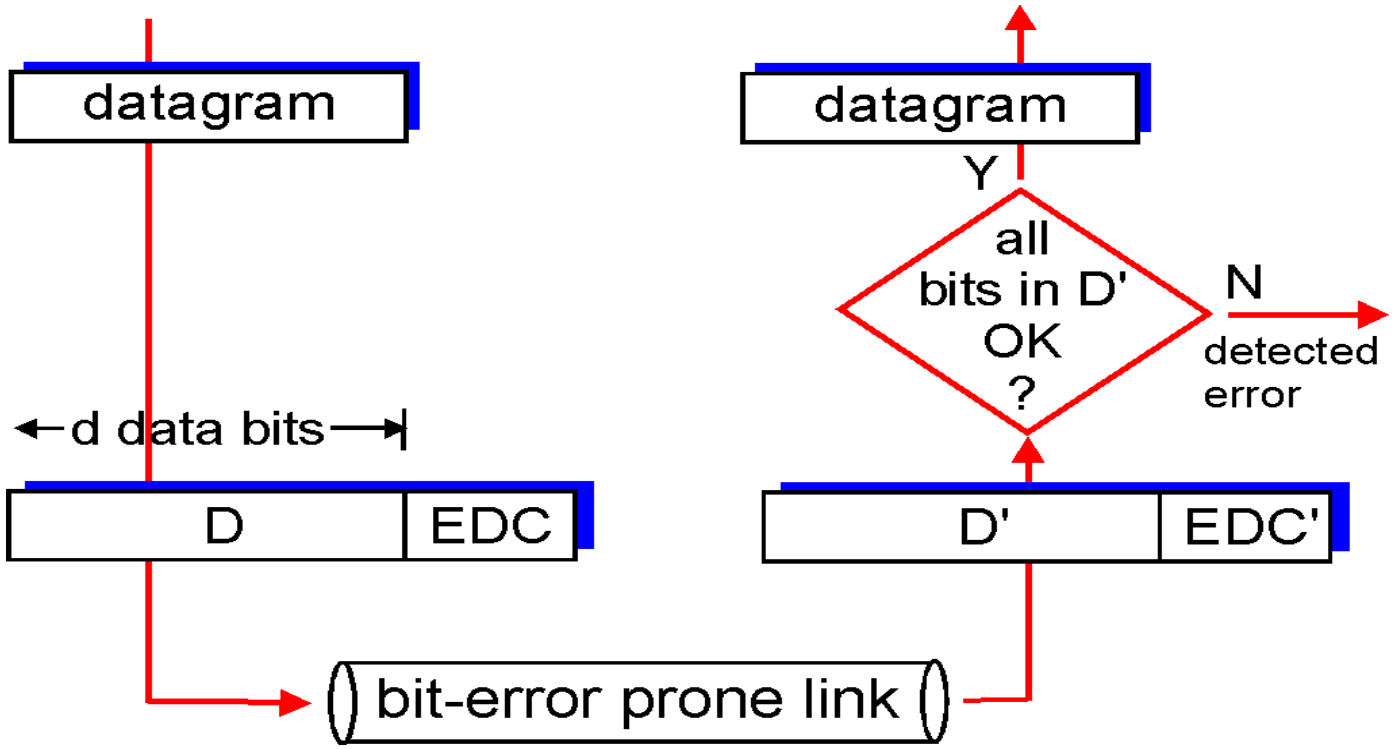


Detección y corrección de errores

- ¿Qué son errores?
  - La señal que representa los bits de la trama, al ser transmitida por la capa física, sufre diversas modificaciones (atenuación, deformación, interferencia, ruido, etc)
  - El receptor puede interpretar erróneamente uno o mas bits del mensaje
- Distintas capas físicas tienen distintas probabilidades de error
- También pueden variar las características de los errores (por ejemplo errores en ráfagas vs. errores independientes)
- Se agrega redundancia para intentar detectar (o eventualmente corregir) estos errores
- Ningún mecanismo puede detectar el 100% de los errores

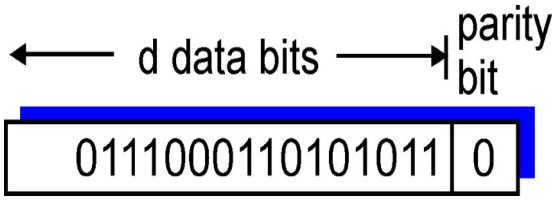
Detección de errores

- Dado un mensaje de largo *d* bits, se le agregan *r* bits de redundancia o chequeo (EDC=Error Detection Code)
- Se transmiten *n=d+r* bits
- El receptor recibe los *n* bits, y verifica la redundancia
- Si detecta un error descarta el mensaje, en caso contrario pasa la carga útil a la capa superior.



Ejemplo: bit de paridad

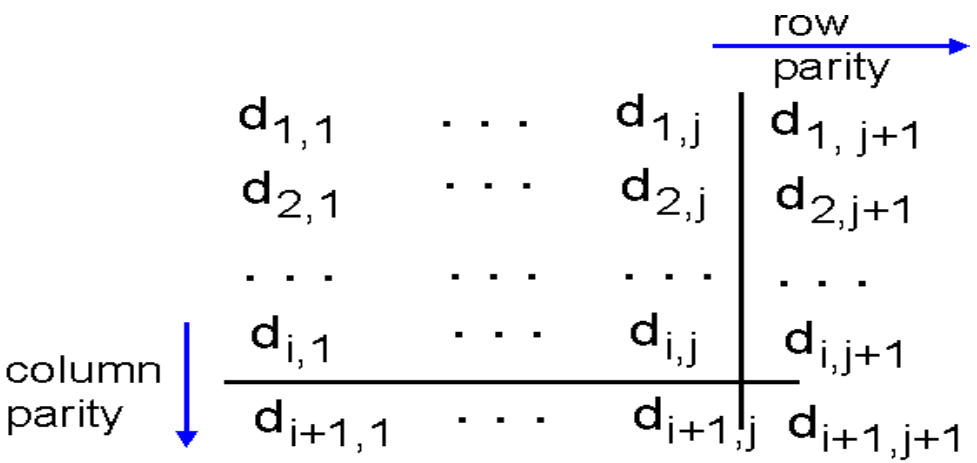
- Se agrega 1 bit (paridad)
- Paridad par: transmisor elige el bit de paridad de forma que la cantidad de bits en 1 sea par (idem paridad impar)
- En el receptor se verifica la paridad
  - En caso de error se descarta
- Detecta todos los errores de 1 bit
- Observar que detecta todos casos con un número impar de bits errados
  - Y ninguno con número par

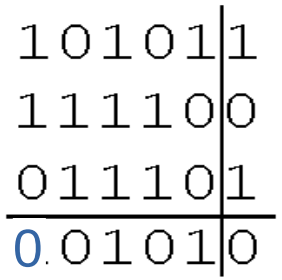


Paridad impar

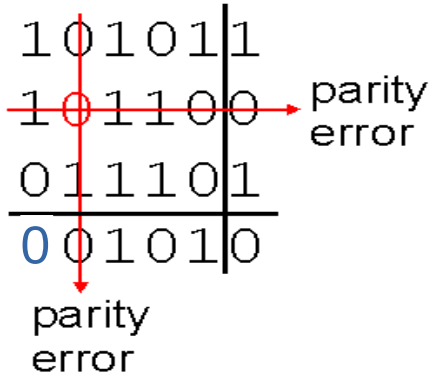
Ejemplo: generalización de paridad en forma matricial

- Bits se organizan en una matriz
- Se calcula bit de paridad para cada fila y columna
- Si asumimos un solo bit errado, podemos determinar qué bit es el errado y corregirlo
  - FEC: Forward Error Correction





no errors



correctable single bit error

Sumas de comprobación

- Se tratan los datos a enviar como enteros de k bits
- Se realiza una cuenta sobre estos enteros
- Ejemplo: suma de comprobación en TCP
  - Se trata los datos como enteros de 16 bits
  - Se realiza la suma
  - Se envía el complemento a 1 de dicha suma
  - En el receptor se verifica
- Fácil de calcular en software
- Bajo overhead
- Protección débil contra errores

Códigos de Redundancia Cíclica (Códigos polinomiales)

- CRC: Cyclic Redundancy check Code (código de redundancia cíclica)
  - También llamados códigos polinomiales
- Muy utilizado en capa 2 (ejemplos: Ethernet, WiFi)
- Mayor capacidad de detección de errores, especialmente errores en ráfagas
- El cálculo es más complejo en software que una suma de comprobación
  - Pero no es un problema si se implementa en hardware
  - Ni es un problema en procesadores modernos

Códigos polinómicos (CRC)

- Se tratan los bits del mensaje como coeficientes de un polinomio
- Si tengo un mensaje de k bits, $c_{k-1}c_{k-2}...c_0$ lo puedo ver como un polinomio de grado k-1
  - $c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + ... + c_0x^0$
- Ejemplo:
  - La secuencia de bits **110001** se representa como:
  - $\mathbf{1}.x^5 + \mathbf{1}.x^4 + \mathbf{0}.x^3 + \mathbf{0}.x^2 + \mathbf{0}.x^1 + \mathbf{1}.x^0$
  - o sea: $x^5 + x^4 + x^0$
  - o sea: $x^5 + x^4 + 1$
- La aritmética se hace en módulo 2, no hay acarreos y tanto la suma como la resta son idénticas al XOR (or exclusivo)
  - 0 + 0 = 0
  - 0 + 1 = 1
  - 1 + 0 = 1
  - 1 + 1 = 0

Códigos polinómicos (CRC)

- El transmisor y receptor deben ponerse de acuerdo en el uso del llamado polinomio generador G(x)
- Los coeficientes más y menos significativos de G(x) deben ser 1
- El mensaje de m bits se representa como D(x) y la trama a transmitir es más larga que el largo de G(x)
- La idea es agregar una suma de comprobación al final de la trama de modo tal que el polinomio representado por el conjunto sea divisible entre G(x)
- El receptor divide lo que recibe entre G(x), si el resto es 0 no hay errores. Si es distinto de 0 es porque hubo errores en la transmisión

Algoritmo para cálculo del CRC de forma polinomial

- Si r es el grado de G(x), agrego r bits en 0 en la parte menos significativa de la trama. Lo que tengo entonces es la representación de

  $x^r\ D(x)$

- Ejemplo:
  - Si tengo la secuencia **110001** que es el polinomio $D(x) = x^5+x^4+1$
  - Y agrego 3 ceros a la derecha, queda **110001000**
  - Quedaría el polinomio: $\mathbf{1}.x^8+\mathbf{1}.x^7+\mathbf{0}.x^6+\mathbf{0}.x^5+\mathbf{0}.x^4+\mathbf{1}.x^3+\mathbf{0}.x^2+\mathbf{0}.x^1+\mathbf{0}.x^0$
  - O sea: $x^8+x^7+x^3$
  - O sea: $(x^5+x^4+1)\ x^3$
  - O sea: $x^3\ D(x)$
- Divido $x^r\ D(x)$ entre G(x) con aritmética módulo 2 y obtengo un resto R(x) (con menos de r bits)
- Resto R(x) a $x^r\ D(x)$ obteniendo $M(x)= x^r\ D(x)-R(x)$ que obviamente es divisible entre G(x)
- Se envía un mensaje cuyos bits son los coeficientes de M(x)

Procesamiento en el receptor

- El receptor recibe un mensaje, M'(x) = M(x) + E(x)
- E(x) representa los errores introducidos en el canal.
  - Tenemos un bit 1 en la posición de cada bit que se haya invertido
    - Si el original era un 0 y le sumo un 1, queda un 1 (error)
    - Si el original era un 1 y le sumo un 1, queda un 0 (error)
- El receptor divide (M(x)+E(x))/G(x) y calcula el resto de la división
- Como:

  Resto[(M(x)+E(x))/G(x)] = Resto[M(x)/G(x)] + Resto[E(x)/G(x)]

  y Resto[M(x)/G(x)] = 0

  => el resultado es Resto[E(x)/G(x)]
- El receptor aceptará como válidos los mensajes que cumplan que el resto calculado es cero (es decir, que son divisibles entre G(x))
- Solo se escapan los patrones de error que correspondan a un polinomio divisible entre G(x)

Códigos polinómicos

- El problema pasa a ser entonces elegir adecuadamente el polinomio G(x)
- Se hace en base a propiedades de los polinomios, por ejemplo:
  - Para detectar error simple: $E(x)=x^i$ (*)
    - se necesita que G(x) tenga al menos dos términos
  - Para detectar dos errores: $E(x)=x^i+x^j=x^j(x^{i-j}+1)$
    - Si G(x) no es divisible por x (condición *)
    - se necesita que G(x) no divida a x^k+1 para cualquier k<i-j (largo de la trama)
  - etc.

Polinomios generadores estandarizados

- Múltiples polinomios generadores estandarizados. Algunos ejemplos:
  - CRC-16 (16 bits) $x^{16}+x^{15}+x^{2}+1$
  - CRC-CCITT (16 bits) $x^{16}+x^{12}+x^{5}+1$
  - IEEE 802 CRC-32 (32 bits)
    $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x^{1}+1$
- Los de 16 bits detectan:
  - 100% simples y dobles
  - 100% los de número impar de bits
  - 100% de ráfagas de largo 16 o menos
  - 99.99% de ráfagas de 17 bits o más bits
- El de 32 bits:
  - 100% simples, dobles y triples
  - 100% los de número impar de bits
  - 100% de ráfagas de largo 32 o menos
  - 99,99999998% de los errores de 4 bits, y otras propiedades

Corrección de errores

- La capacidad de detectar y **corregir** errores en el receptor se denomina “Forward Error Correction” (FEC)
- Requieren un overhead sustancialmente mayor que los códigos detectores de error
- No estudiaremos ninguno de ellos en particular.
- Se utilizan:
  - En medios con alta tasa de error, donde se justifica el overhead para evitar una retransmisión
  - En enlaces con un delay muy grande que hace impráctica la retransmisión
  - Otras aplicaciones, como el almacenamiento de datos en discos magnéticos, CDs y DVDs, donde la “retransmisión” no es posible

Entrega confiable

- Algunos protocolos de capa de enlace ofrecen el servicio de entrega confiable
- ¿Por qué tener entrega confiable en capa de enlace, si la tenemos en capa de transporte?
  - Evitar la retransmisión end to end para links con alta probabilidad de errores (se retransmite sólo en el tramo donde falla)
  - Capas de transporte sin entrega confiable
  - Etc.
- Se utilizan los mismos principios que vimos en capa de transporte
  - Ventanas deslizantes, reconocimientos
  - Repetición selectiva o go back N
- Muchos protocolos sobre enlaces con baja tasa de errores (fibra, par trenzado) no implementan servicios de entrega confiable
- Algunos protocolos lo implementan parcialmente: se implementan reconocimientos (garantiza entrega) pero sin ventanas deslizantes (pueden generar duplicados por pérdida del reconocimiento)

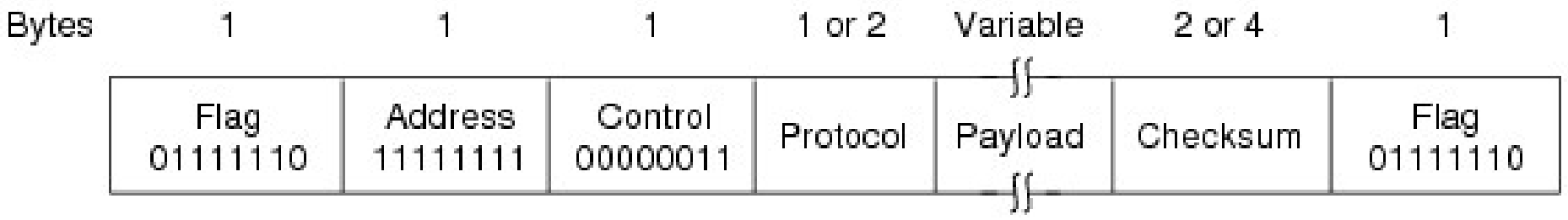
Control de flujo

- El control de flujo en capa de enlace cumple la misma función que en capa 4
  - Pero entre equipos adyacentes, no punta a punta
- Se implementa de la misma manera que en capa de transporte, utilizando ventanas deslizantes
- En los protocolos de redes de área local (Ethernet, WiFi) no se suele utilizar control de flujo
  - En versiones recientes de Ethernet existe una opción de “solicitud de pausa” para cumplir esta función

Ejemplo de protocolo de capa de enlace: PPP

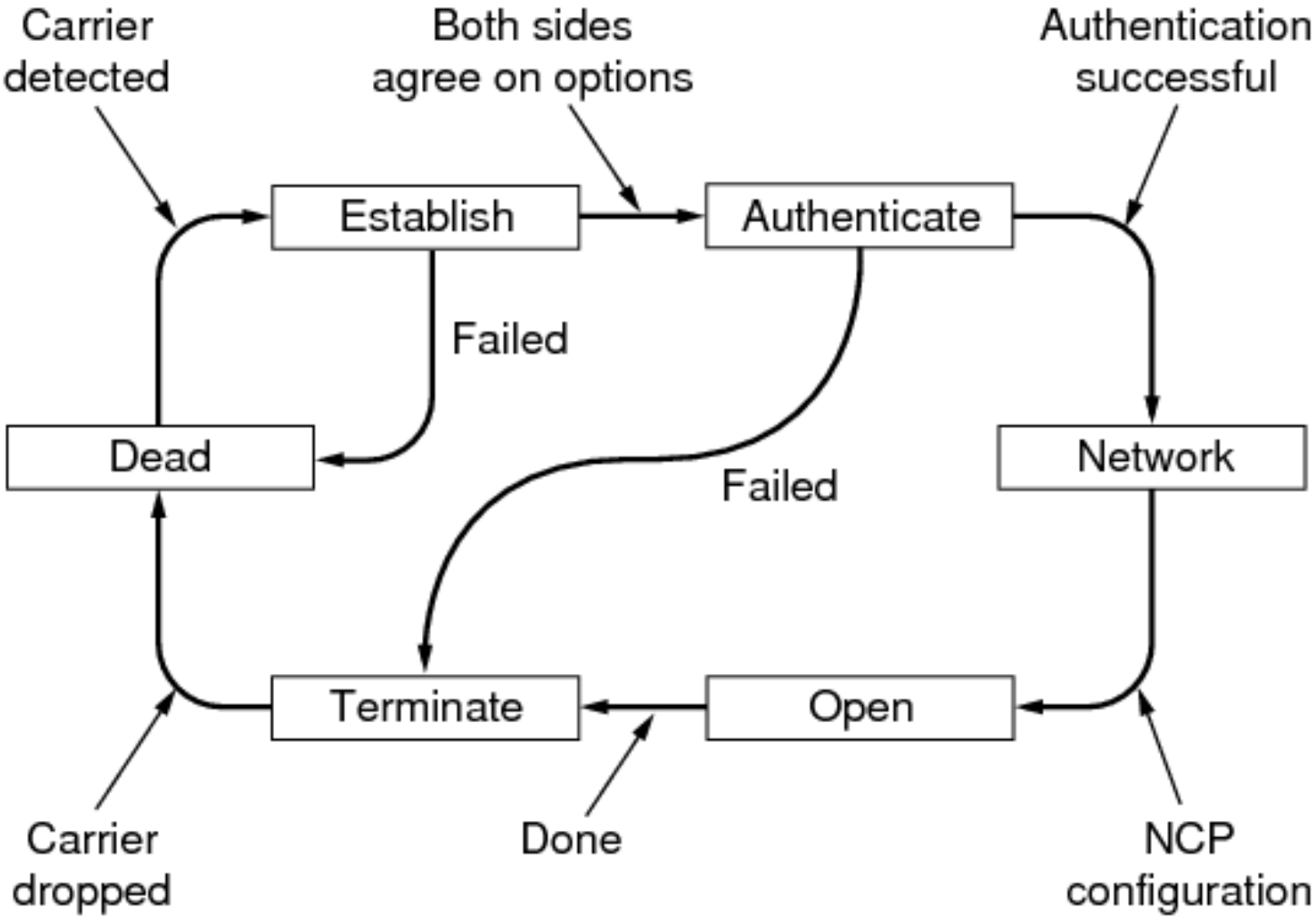
- PPP (Point to Point Protocol): protocolo para enlaces punto a punto
- Provee:
  - Entramado (framming) con detección de error
  - LCP (Link Control Protocol): para conectarse, testear la línea, negociar opciones y terminar una conexión
  - NCP (Network Control Protocol): una manera de negociar opciones a nivel de capa de red (por ej. la dirección)

- Formato de trama:



- Utiliza relleno de bits si aparecen secuencias de más de 5 “1” en el payload

PPP: Diagrama de estados simplificado



Capa de enlace
Sub capa de acceso al medio

Facultad de Ingeniería – Universidad de la República

Agenda

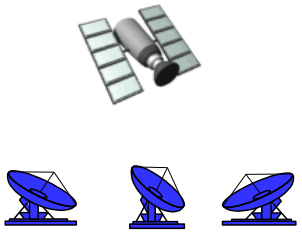
- Conceptos de capa de enlace
  - Objetivo y funciones de la capa de enlace
  - Entramado
  - Detección y corrección de errores
  - Servicios confiables
- Ejemplos de protocolos punto a punto
- Protocolos de acceso a medios compartidos
  - Protocolos para compartir el canal
- Redes de área local cableadas
  - 802.3 y su evolución
  - Redes con switches
  - Vlans
- Redes de área local inalámbricas
- Networking en el datacenter

Sub Capa MAC (Medium Access Control)

- Aparece cuando tenemos un medio donde múltiples estaciones pueden transmitir (y recibir) tramas
  - También se les suele llamar redes broadcast (una trama enviada llega a todos los receptores)
- Nuevos problemas a resolver:
  - Coordinar el acceso al medio
  - Seleccionar el destino
- Algunos ejemplos:

Cable compartido (ej., Ethernet tradicional)

RF compartido (ej., 802.11 WiFi)



RF compartido (satélite)

Personas en una fiesta (aire compartido, acústico)

Sub capa MAC

- Objetivo (original): compartir un mismo canal entre múltiples estaciones
  - Eficientemente
  - De forma sencilla
  - “económicamente”
- Requeriremos:
  - Direccionamiento de las estaciones
  - Mecanismo para compartir el canal
  - En general se utiliza solamente detección de errores (porque el canal tiene relativamente poca tasa de error)

Direccionamiento en capa MAC

- Necesidad: separar el tráfico de diferentes estaciones
  - Solamente tomar “mis” tramas
  - La tarjeta descartará el tráfico no dirigido a mi
  - Ahorro procesamiento en la CPU
- Los switches podrán enviar la trama al puerto adecuado
- Dirección asociada a la interfaz de red
- Sólo significado local al medio compartido

- Distintos protocolos elegirán distintas direcciones
- En general, división en direcciones unicast (una estación), multicast (un grupo) y broadcast (todas las estaciones)
- En los protocolos LAN desarrollados por la IEEE, direcciones MAC de 48 bits
  - Las veremos luego

¿Por qué otras direcciones?

- ¿Por qué no compartir las direcciones con la capa de red?
- Independencia de capas
  - ¿Las direcciones de cuál protocolo de red?
    - IP no es el único protocolos de capa de red
  - ¿Cómo manejo 2 protocolos de red sobre la misma capa MAC?
- Direccionamiento global (capa 3) versus local (capa 2)
  - Distintos objetivos requieren soluciones distintas

2 tipos de medios broadcast

- Canales compartidos físicamente:
  - Estaciones utilizan el mismo medio físico
  - Posibilidad de “interferencia”
  - Ejemplo: redes inalámbricas, 802.3 original
- Canales compartidos lógicamente:
  - A nivel físico las estaciones tienen enlaces punto a punto con un concentrador o switch
    - No hay posibilidad de “interferencia”
  - Pero a nivel lógico cada estación puede enviar tramas a cualquier otra (o a todas) las que comparten el dominio de broadcast
  - Ejemplo: ethernet switcheada (la veremos luego)
  - En este caso también tenemos una capa MAC

Características deseables en un protocolo MAC

- Equitativo
  - Dado un canal de R bits por segundo:
    - Cuando un solo nodo quiere transmitir, puede utilizar toda la capacidad de R bps
    - Si M nodos quieren transmitir, cada uno puede hacerlo a una velocidad promedio de R/M bps
- Un protocolo descentralizado
  - No requiere un nodo especial para coordinar las transmisiones
  - No requiere sincronización de relojes ni de timeslots
- Simple

Taxonomía de los protocolos de capa MAC

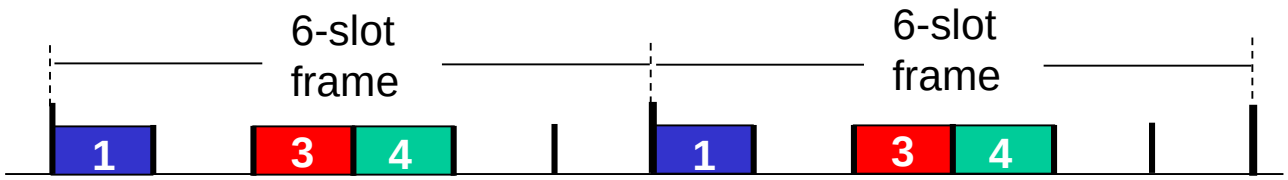
- Hay 3 grandes clases:
  - Particionado del canal:
    - Se divide el canal en fracciones (frecuencia/tiempo/código)
    - Se asigna una fracción a cada nodo para su uso exclusivo
  - Acceso aleatorio:
    - Canal no se divide
    - Se permiten colisiones entre estaciones que transmiten a la vez
    - Debemos poder “recuperarnos” de las colisiones
  - “Nodos se turnan”
    - Los nodos toman turnos para transmitir
    - Los nodos que tienen más para transmitir pueden tomar turnos más largos
- Además de las clases anteriores, podemos considerar una “sub-clase” donde los nodos se conectan a un dispositivo, “switch”, que se encarga de reenviar las tramas entre segmentos.

Colisiones

- Cuando dos tramas se superponen en el tiempo (en el mismo canal), se dice que hay una colisión
- El receptor recibe la superposición de varias señales, que no podrá distinguir
- Las tramas que colisionan son irrecuperables. No es posible determinar las tramas originales observando el canal
- El receptor se da cuenta ya sea porque a nivel de capa física/MAC se violan las restricciones del protocolo, o porque no verifica la suma de comprobación (CRC)

Protocolos MAC particionando el canal: TDMA

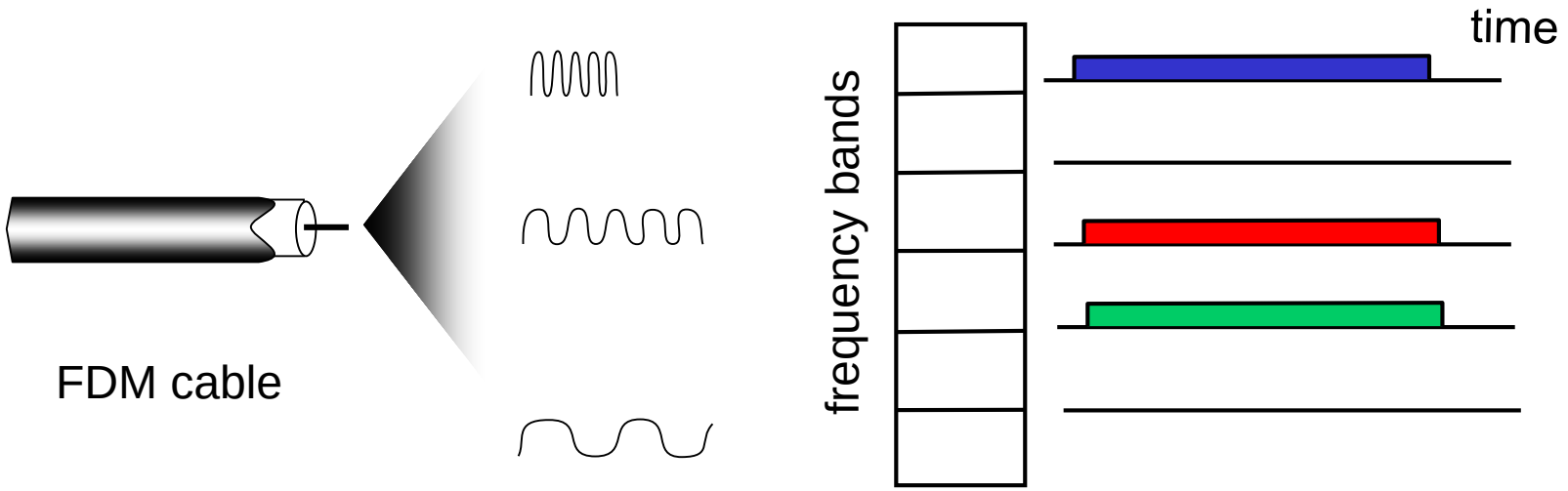
- TDMA: Time Division Multiple Access
  - Acceso al canal en “rondas”
  - Cada estación recibe un slot de tiempo fijo en cada ronda (por ejemplo el tiempo necesario para enviar una trama de tamaño máximo)
  - Si una estación no tiene datos para transmitir su slot se desperdicia
  - Ejemplo, 6 estaciones:



- Defecto: si muchas estaciones tienen tráfico esporádico, se desperdicia mucha capacidad
- Ventaja: no hay colisiones

Protocolos MAC particionando el canal: FDMA

- FDMA: Frequency Division Multiple Access
- Se divide el espectro disponible en múltiples bandas, asignando una a cada estación
- Al igual que en TDMA, se desperdicia la capacidad correspondiente a las estaciones que no tienen datos para transferir



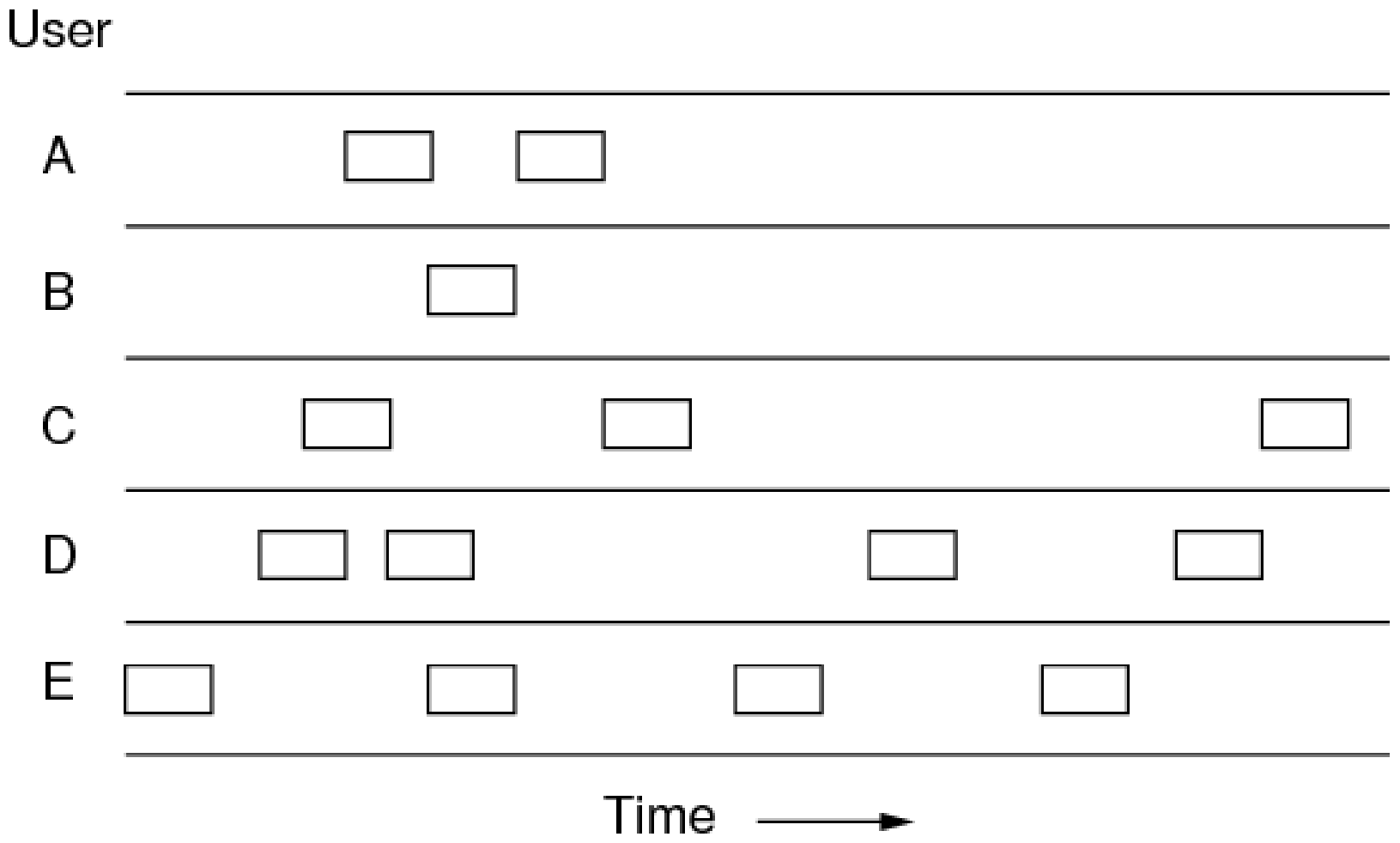
Link Layer and LANs 6-22

Protocolos con acceso aleatorio

- Cuando un nodo tiene algo para transmitir:
  - Transmite usando la capacidad completa del canal R (cumpliendo ciertas reglas)
  - No hay una coordinación a-priori entre los nodos
- Si dos o más nodos transmiten, hay una colisión
  - Precisamos poder detectar las colisiones
  - Precisamos poder recuperarnos de las colisiones

Un poco de historia: ALOHA

- 1970 radio bases en Hawaii (Abramson)
- Estaciones transmiten cuando tienen datos
  - Sin ninguna coordinación

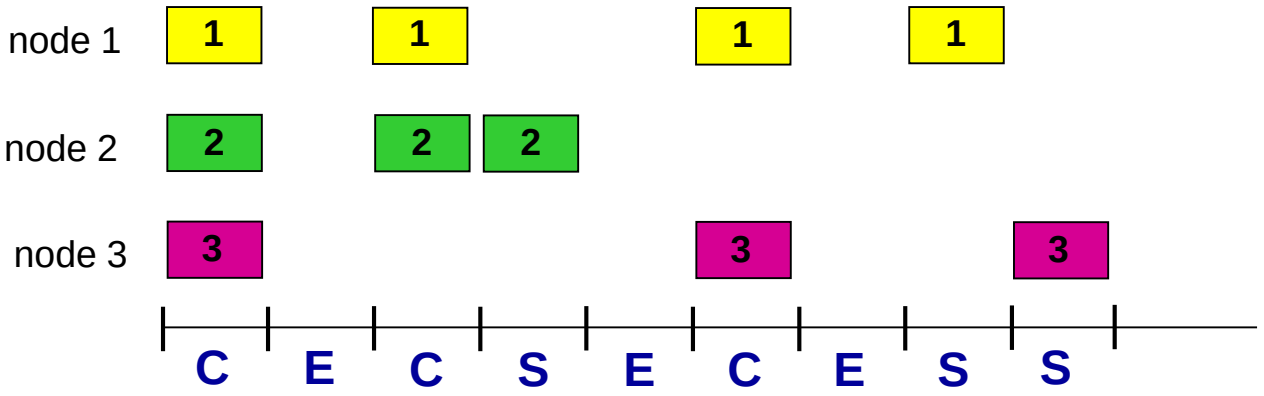


ALOHA (2)

- se detecta si hubo colisión
  - Variantes: inmediatamente o con retardo
  - En el original, observo si me retransmiten mi trama
- En caso de colisión, se debe esperar un tiempo aleatorio y retransmitir
  - **Debe ser aleatorio para evitar la sincronización entre las estaciones**
- Eficiencia teórica máxima posible: 18%

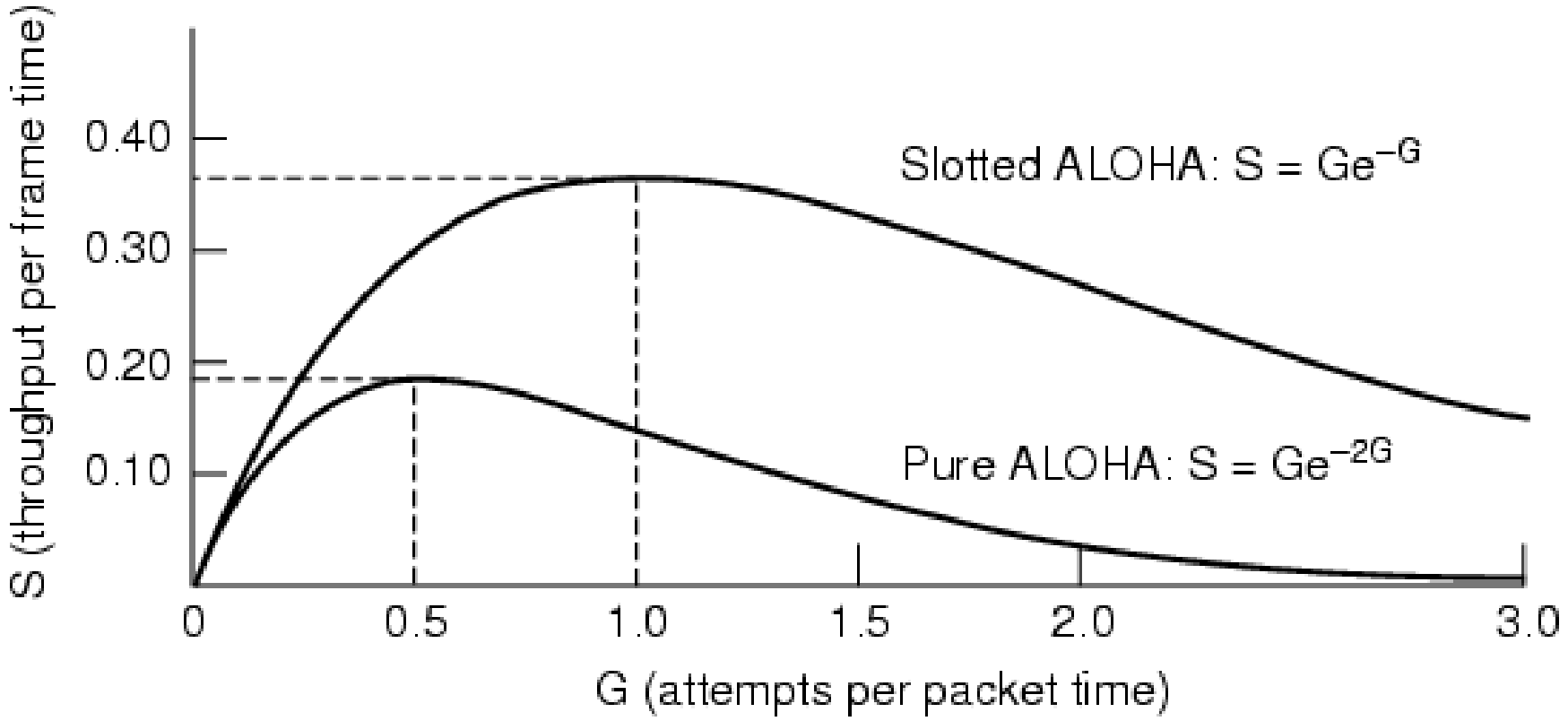
ALOHA ranurado

- 1972: se discretiza el tiempo (slots o ranuras de tiempo de duración necesaria para transmitir una trama)
- Solo puedo transmitir al comienzo de un slot
- Problema: preciso sincronización entre estaciones
- Si 2 o más estaciones transmiten en el mismo slot, todas las estaciones se dan cuenta de la colisión
- Si hay una colisión, esperan un tiempo aleatorio



Eficiencia (modelo simplificado)

- Pueden ver el cálculo en el libro (Kurose o Tanenbaum)
- En la gráfica se observa el promedio de utilización del canal (proporción de slots con tramas útiles) en función de la carga ofrecida (G)



Protocolos con detección de portadora (CSMA)

- CSMA: Carrier Sense Multiple Access (Acceso Múltiple con detección de portadora)
- Mejora: Antes de transmitir, detectar si otro equipo está utilizando el canal (“portadora”)
- Igual hay colisiones por retardos de propagación en el canal
  - Escucho libre el canal por más que el otro comenzó a transmitir
- Solo utilizables en medios con bajo retardo, donde las estaciones puedan “escucharse entre sí en tiempo real”

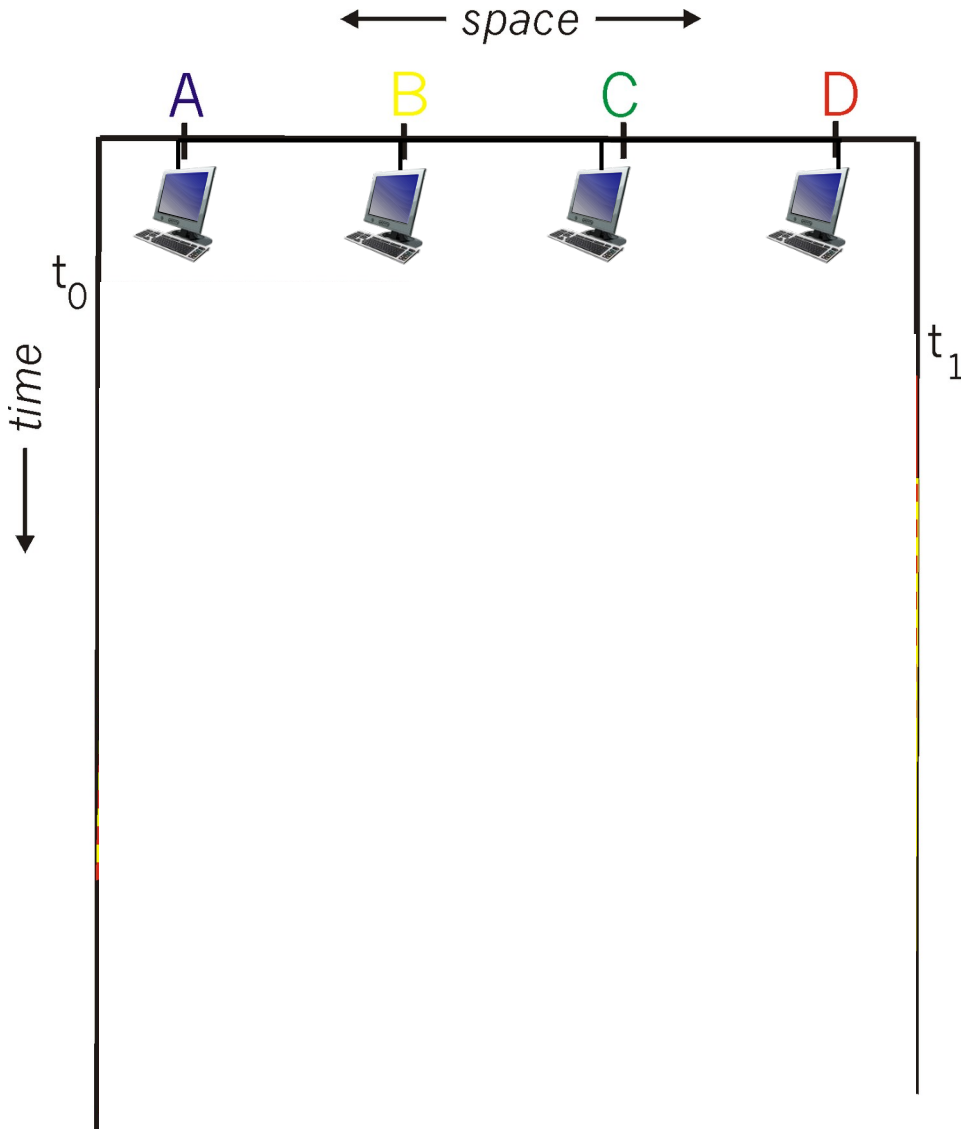
Colisiones en CSMA

- Pueden ocurrir colisiones

  El retardo de propagación hace que los nodos puedan no escucharse a tiempo

- En caso de colisión, se desperdicia todo el tiempo correspondiente a la transmisión de una trama

- La probabilidad de colisión aumenta con la distancia entre estaciones



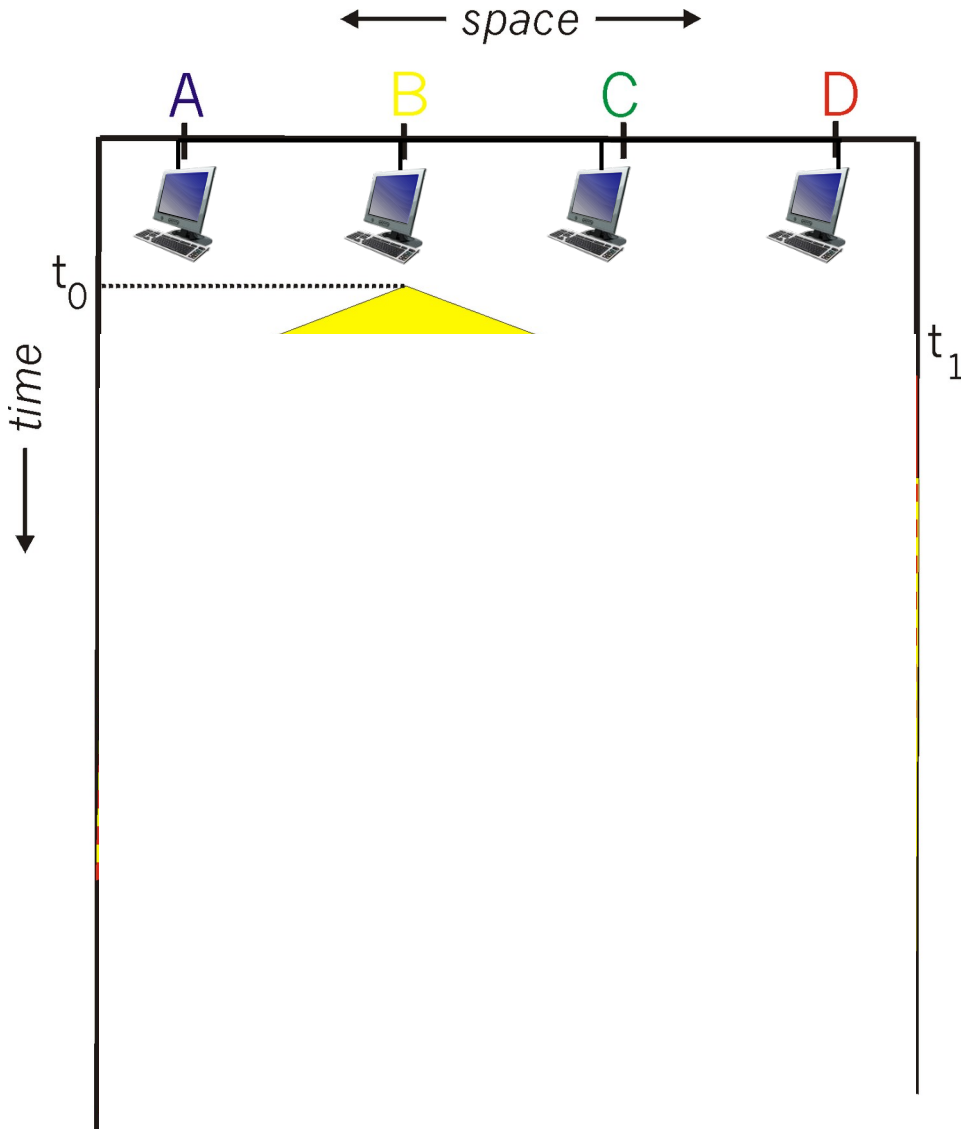
Colisiones en CSMA

- Pueden ocurrir colisiones

  El retardo de propagación hace que los nodos puedan no escucharse a tiempo

- En caso de colisión, se desperdicia todo el tiempo correspondiente a la transmisión de una trama

- La probabilidad de colisión aumenta con la distancia entre estaciones



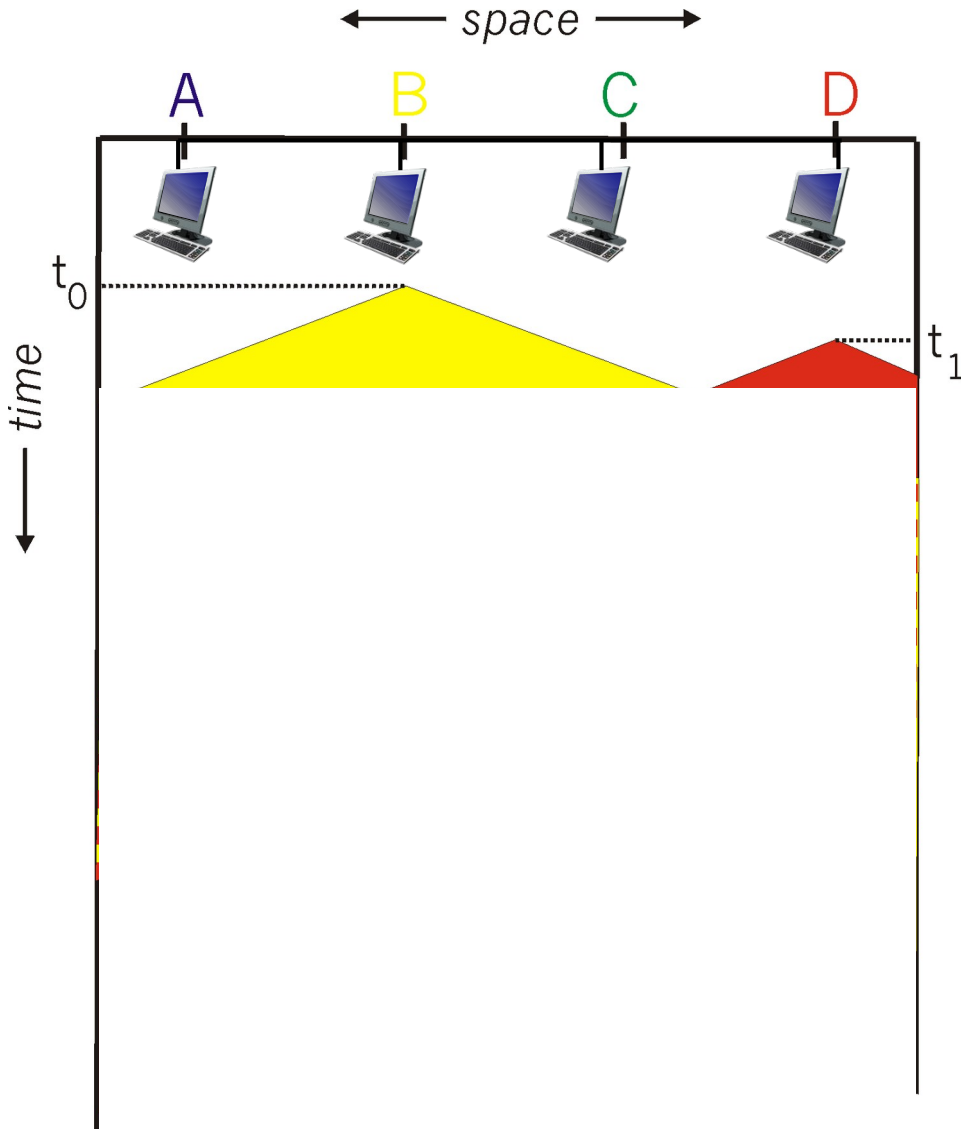
Colisiones en CSMA

- Pueden ocurrir colisiones

  El retardo de propagación hace que los nodos puedan no escucharse a tiempo

- En caso de colisión, se desperdicia todo el tiempo correspondiente a la transmisión de una trama

- La probabilidad de colisión aumenta con la distancia entre estaciones



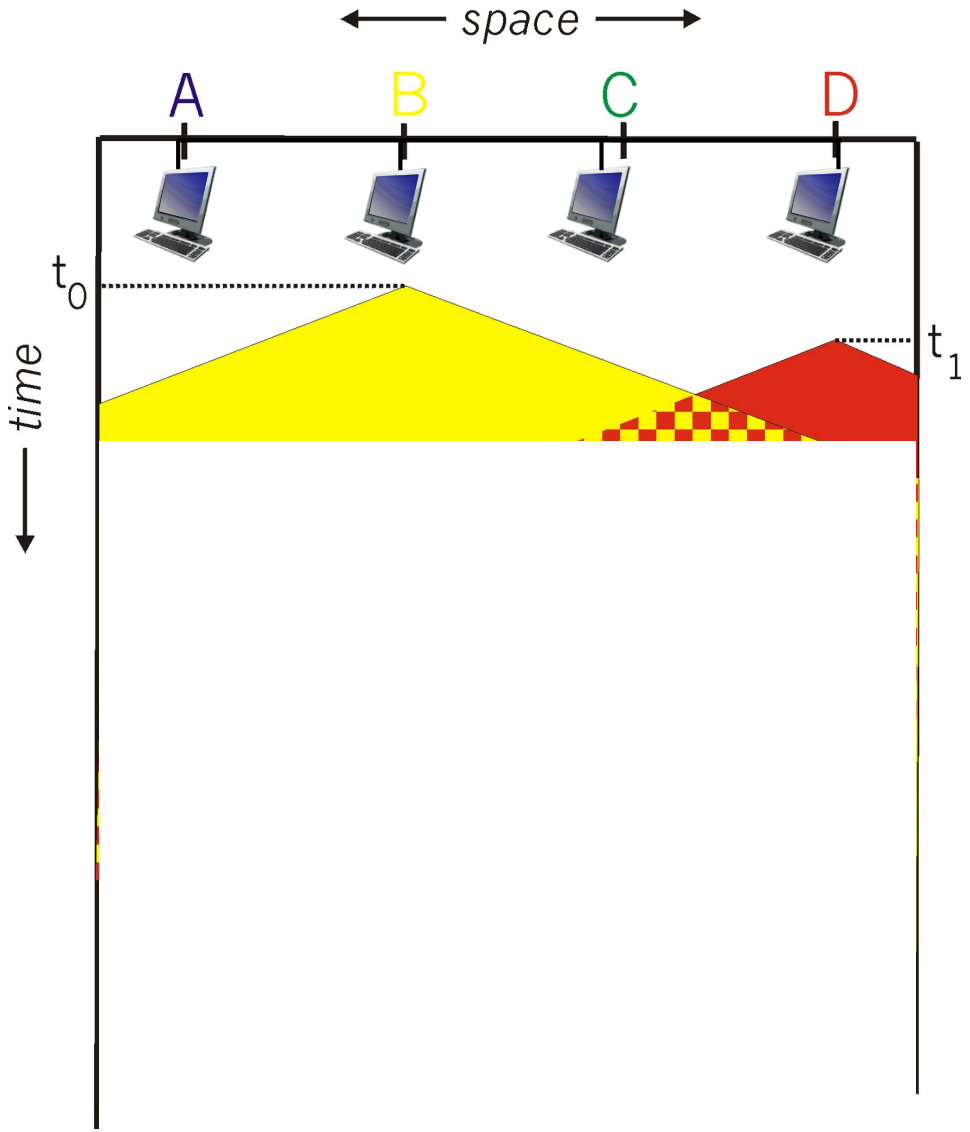
Colisiones en CSMA

- Pueden ocurrir colisiones

  El retardo de propagación hace que los nodos puedan no escucharse a tiempo

- En caso de colisión, se desperdicia todo el tiempo correspondiente a la transmisión de una trama

- La probabilidad de colisión aumenta con la distancia entre estaciones



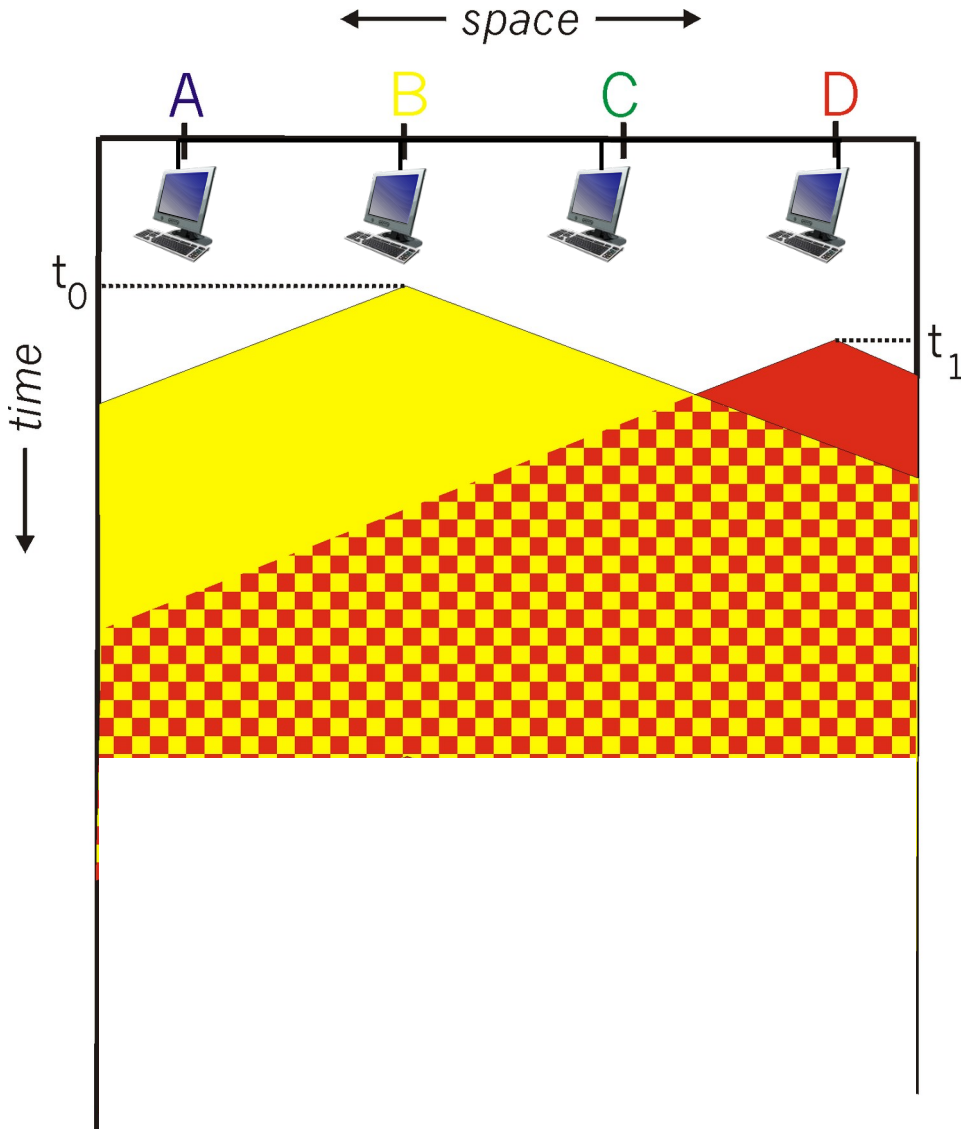
Colisiones en CSMA

- Pueden ocurrir colisiones

  El retardo de propagación hace que los nodos puedan no escucharse a tiempo

- En caso de colisión, se desperdicia todo el tiempo correspondiente a la transmisión de una trama

- La probabilidad de colisión aumenta con la distancia entre estaciones



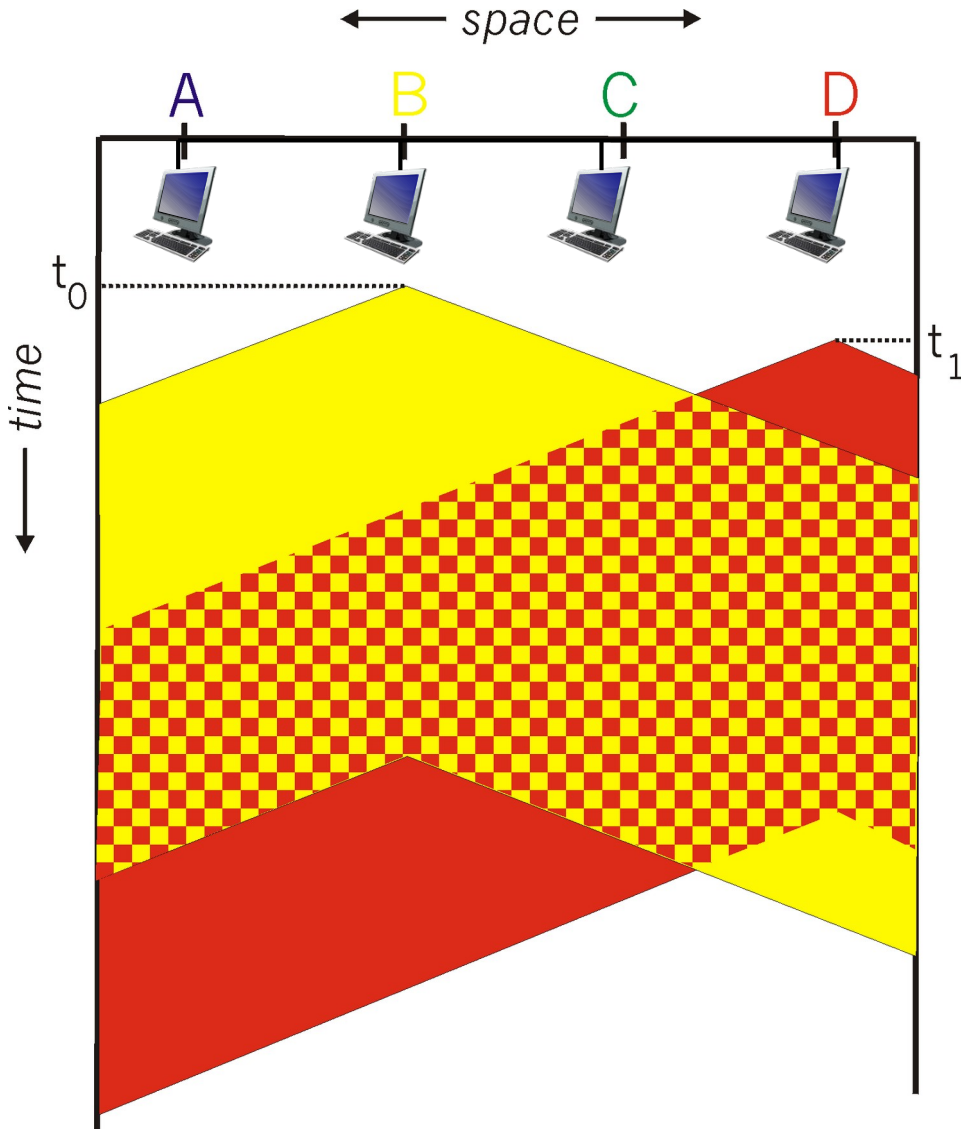
Colisiones en CSMA

- Pueden ocurrir colisiones

  El retardo de propagación hace que los nodos puedan no escucharse a tiempo

- En caso de colisión, se desperdicia todo el tiempo correspondiente a la transmisión de una trama

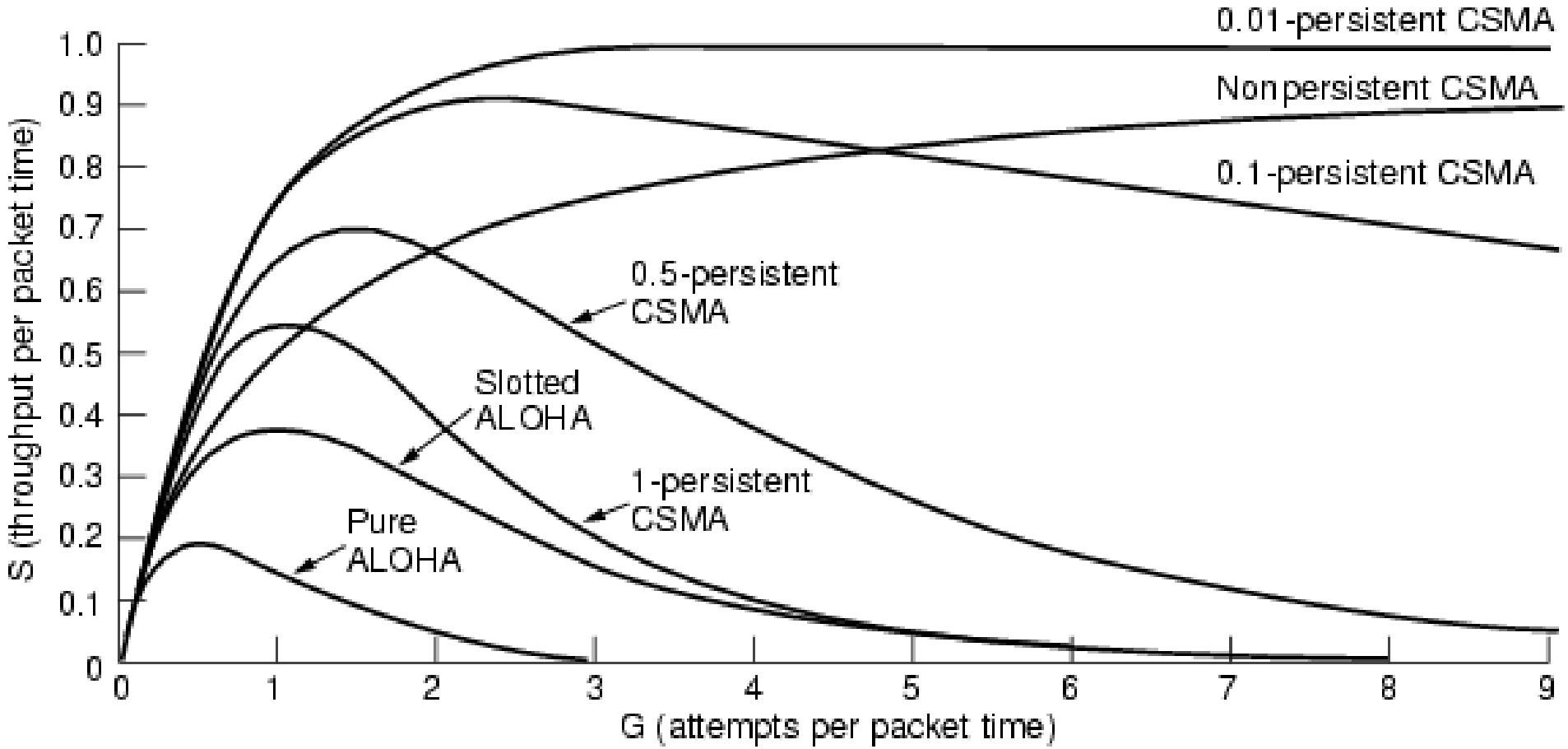
- La probabilidad de colisión aumenta con la distancia entre estaciones



Variantes de CSMA

- CSMA persistente y no persistente
  - persistente o 1-persistente
    - Si el canal esta libre se transmite
    - Si está ocupado, se transmite tan pronto se libere
  - no-persistente
    - Si el canal esta libre se transmite
    - Si el canal está ocupado, se espera un tiempo aleatorio antes de sensar nuevamente el canal
- CSMA p-persistente
  - canales en tiempo ranurado (estaciones sincronizadas)
  - Si el canal está ocupado, se mira el canal en la siguiente ranura
  - Si el canal está libre, transmite con probabilidad p y espera hasta la siguiente ranura con probabilidad 1-p
  - Si el canal se ocupa, se espera un tiempo aleatorio y se comienza nuevamente

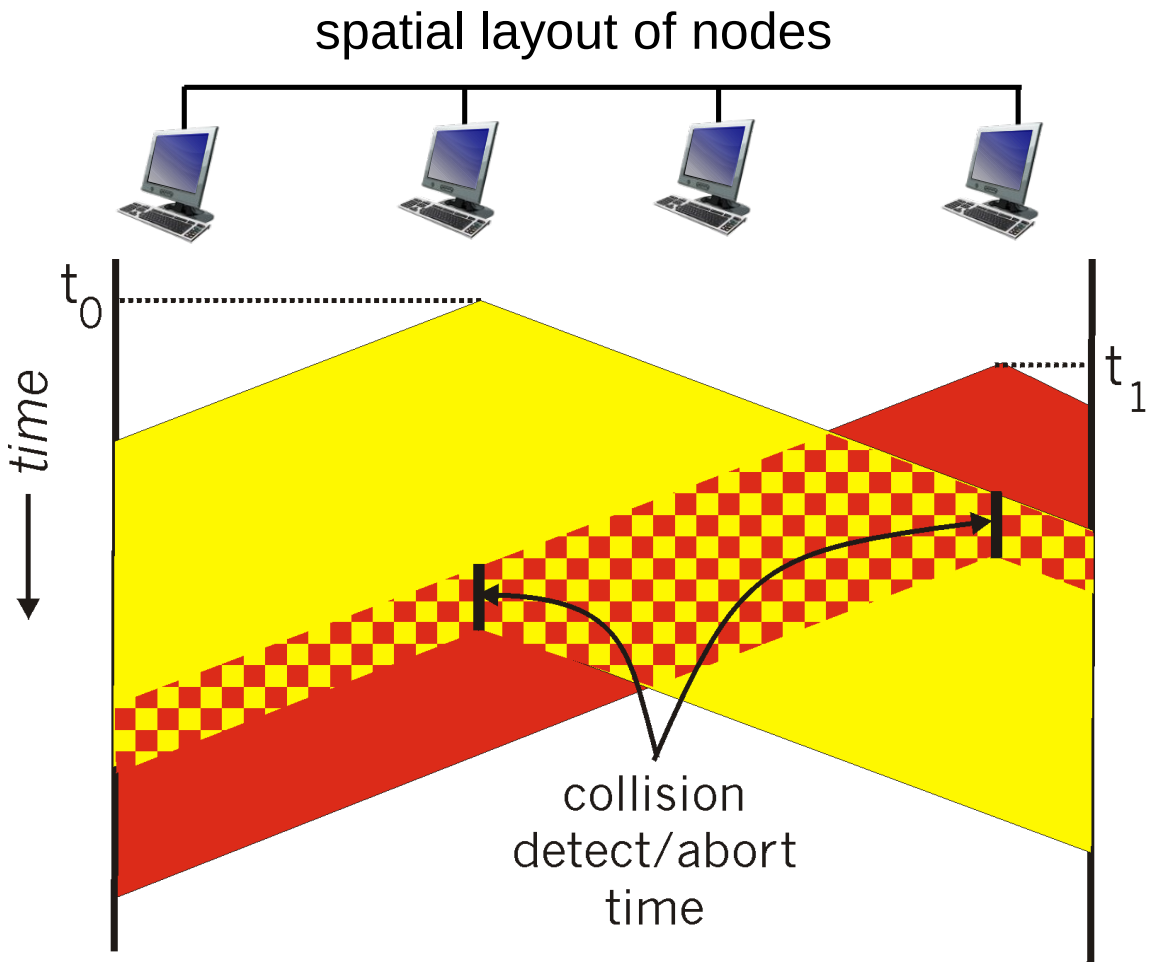
Comparación de performance (modelos simplificados)



CSMA/CD (CSMA con detección de colisión)

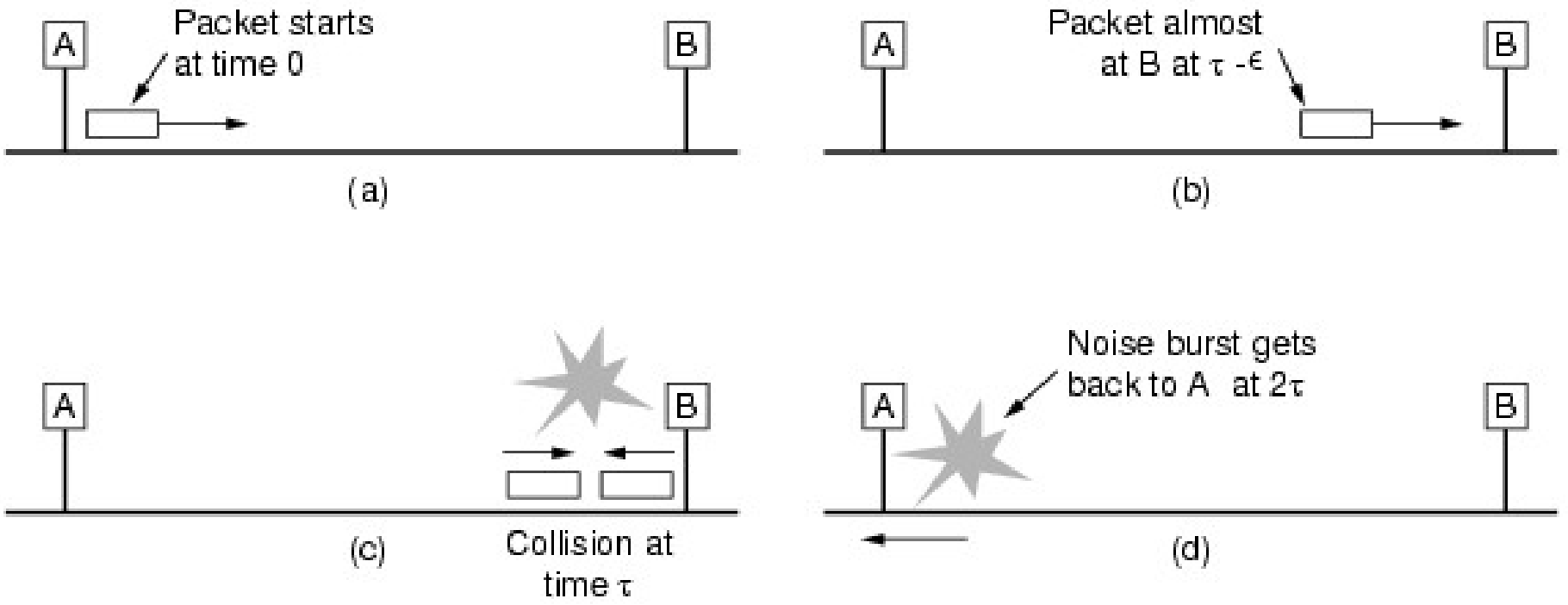
- CD: Collision detection
- Sensar el canal mientras se transmite (escuchar mientras se habla)
- Detener la transmisión cuando detecta colisión
- Detección de colisiones: analógico
  - Se ve si en el canal se lee algo distinto a lo que se escribió
- Ejemplo: Ethernet (802.3) a bajas velocidades (10-100 Mbps) usa CSMA/CD
- No se evitan colisiones, pero se disminuye el tiempo que el canal está ocupado con la colisión

Diagrama espacio/tiempo



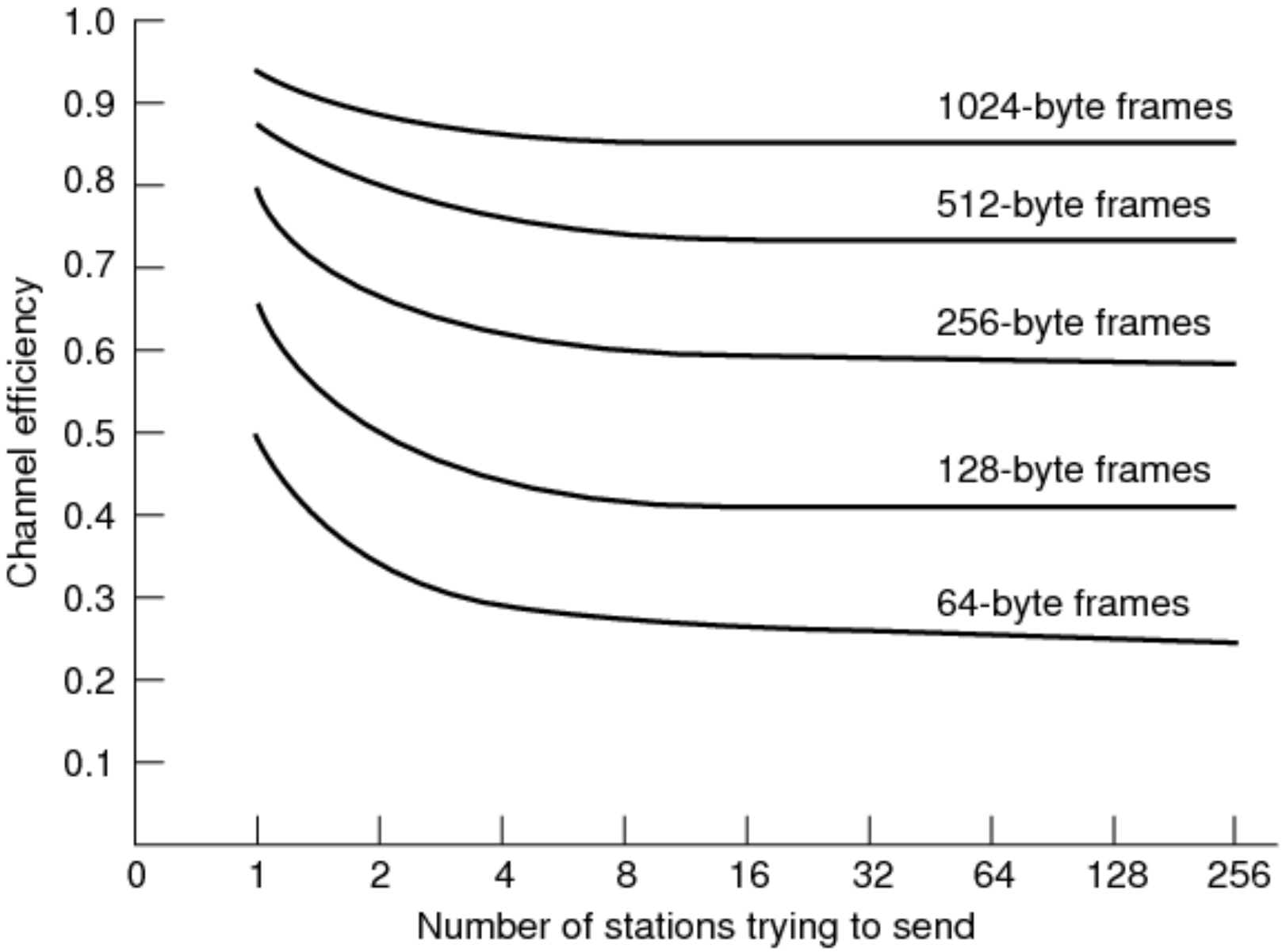
Largo mínimo de trama en CSMA/CD

- Queremos asegurarnos que todos los equipos detectan la colisión



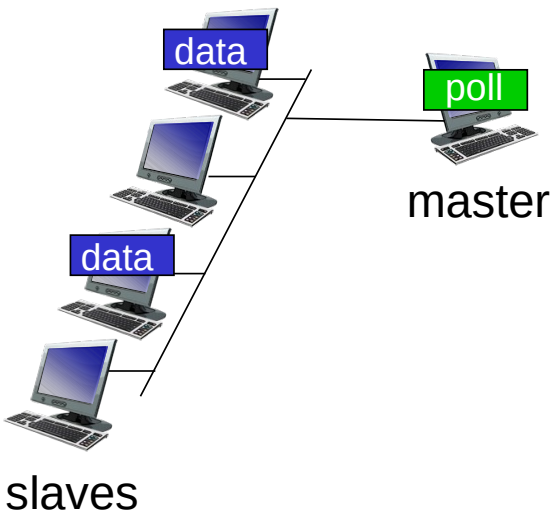
- Si antes que llegue la señal desde B, A deja de transmitir, no tiene forma de saber si la colisión fue con su trama
- Tiempo mínimo de transmisión: 2🔀 (tiempo de ida y vuelta)
- Se impone como mínimo de trama el tiempo de ida y vuelta entre las estaciones más lejanas (precisamos un máximo de distancia permitido)

Eficiencia (modelo simplificado)

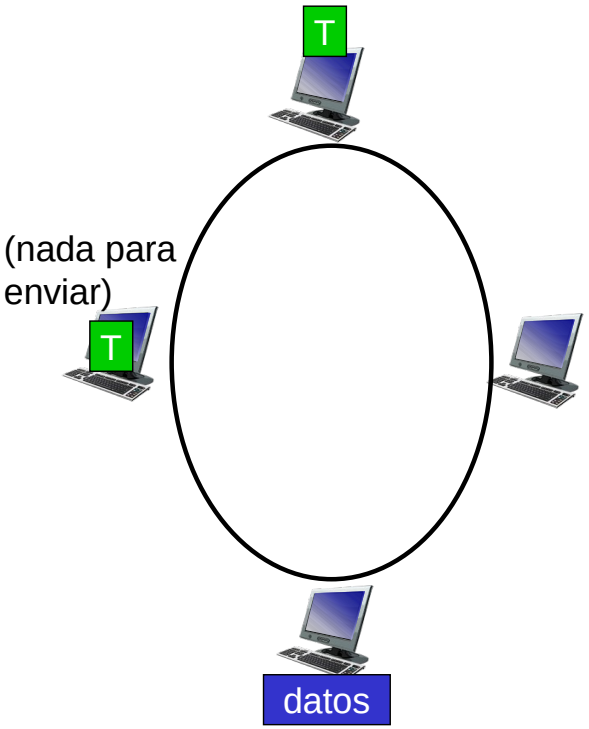


Protocolos “por turnos”

- “polling” (encuesta)
  - Nodo maestro “invita” a cada esclavo a transmitir por turnos
  - Típicamente esclavos “tontos”
  - Problemas: punto de falla (maestro), overhead debido al polling, latencia
  - Ej.: Bluetooth



- Pasaje de token (ficha)
  - Ficha de control se pasa de una estación a la siguiente secuencialmente
  - Sólo se envía si se tiene el token
  - Problemas: recuperación de la ficha si se corrompe, latencia, overhead
  - Redes históricas: Token ring, token bus



Redes de área local

Facultad de Ingeniería – Universidad de la República

Agenda

- Conceptos de capa de enlace
  - Objetivo y funciones de la capa de enlace
  - Entramado
  - Detección y corrección de errores
  - Servicios confiables
- Ejemplos de protocolos punto a punto
- Protocolos de acceso a medios compartidos
  - Protocolos para compartir el canal
- Redes de área local cableadas
  - 802.3 y su evolución
  - Redes con switches
  - Vlans
- Redes de área local inalámbricas
- Networking en el datacenter

Redes de área local (Serie IEEE 802.3)

- 802.1: introducción
- 802.2: LLC
- 802.3: CSMA/CD LAN (Ethernet)
- 802.4: Token bus
- 802.5: Token ring
- 802.11: WiFi (lan inalámbrica)
- 802.15: Redes de área personal (Bluetooth, etc.)
- 802.16: WiMax (MAN inalámbrica)
- Otros

Perspectiva histórica

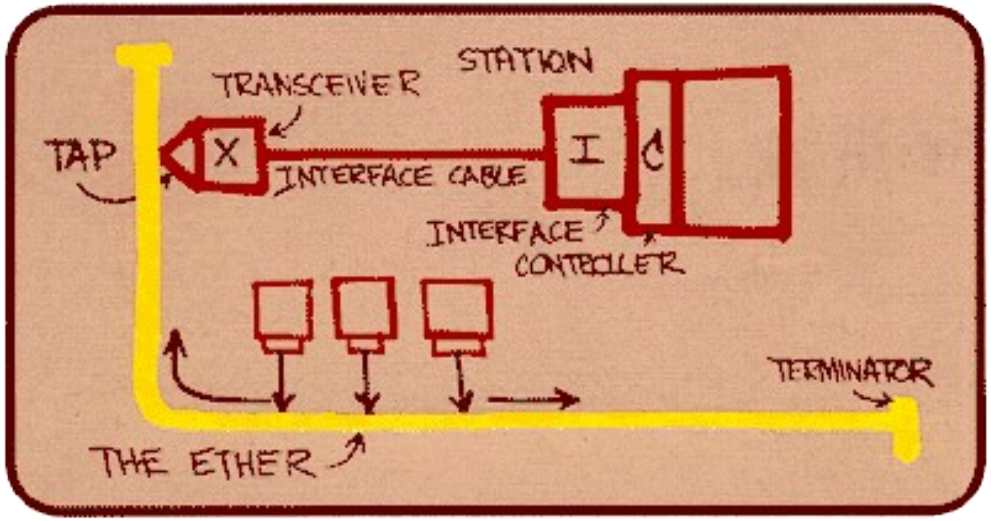
- Las primeras normas de la serie IEEE 802 surgieron a fines de la década de 1970 (802.1 a 802.5)
- 3 grandes grupos de interés, no pudieron conciliar una posición única
  - 3 normas incompatibles entre si
    - Dec, Intel, Xerox: 802.3 (Ethernet)
    - IBM: 802.5. Token Ring
    - General motors: 802.4. Token Bus
  - Solo 802.3 continúa siendo utilizada
- Principales ventajas de 802.3: simplicidad, costo
- A fines de los años 90 se juntaron nuevos grupos para definir una red inalámbrica. En 1997 surgió la primer versión (802.11), seguido por múltiples versiones que fueron mejorando sus prestaciones.
- A principios de los 2000: Redes de área personal (802.15, basada en Bluetooth)
- Muchas otras

Direccionamiento en capa MAC

- En el caso de las redes de área local (Ethernet, WiFi) normalizadas por la IEEE, se utilizan direcciones de 48 bits
  - Ejemplo: 40:8d:5c:18:1b:c7
- Cada tarjeta trae grabada una dirección de fábrica
  - No están relacionadas con la red, sino con el dispositivo
  - Muchas veces se puede cambiar por software
- Todos los bits en 1 : broadcast (todas las estaciones la procesan)
- Direcciones de multidifusión: bit de mayor orden (bit 47) en 1
  - Multidifusión: Solo los equipos interesados en esa dirección la procesan
- Bit 46 en 1: direcciones locales
- Bit 46 en 0: direcciones globales, asignadas por la IEEE
- Asignación de direcciones: coordinada por la IEEE
  - Los fabricantes obtienen de la IEEE un prefijo (24 bits) y fijan el resto de los bits en cada adaptador
  - Me asegura que puedo conectarme en cualquier red sin duplicados

Ethernet (802.3)

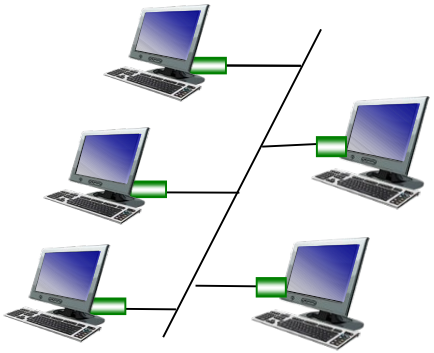
- Ethernet (IEEE 802.3) es el protocolo para redes de área local cableadas más utilizado hoy en día
- Su uso se ha extendido también a las redes de área amplia (WAN)
- Un conjunto de normas y actualizaciones a lo largo de 40 años
- Continúa evolucionando
- Primer versión: Bob Metcalfe y David Boggs (mediados de los 1970)
- Topología en BUS
  - Todas las estaciones se conectan al mismo cable
- Normalizada con mínimos cambios como 802.3



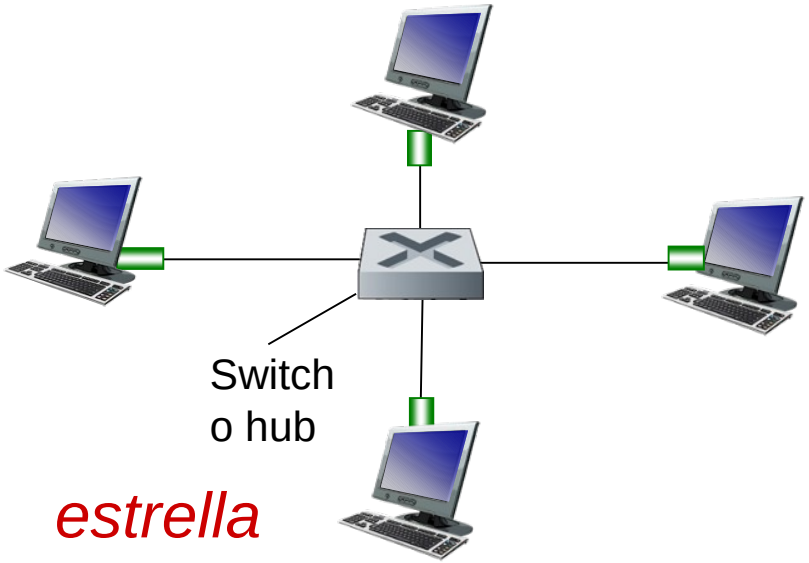
Sketch de la Ethernet de Bob Metcalfe

Topologías físicas de Ethernet

- Bus: común hasta mediados de los años 90
  - Todas las estaciones conectadas al mismo bus físico, colisiones.
  - Bus: cable coaxial
- Estrella: topología hasta nuestros días
  - Cada estación dispone de un medio dedicado hacia switch o repetidor
    - Repetidor: amplifica señales, incluyendo colisiones
  - El medio puede ser par trenzado, o fibra óptica



bus: cable coaxial



estrella

Ethernet original (802.3)

- Protocolo de acceso al medio: CSMA/CD persistente 1
- Velocidad: 10 Mbps
- Medios físicos: Cable coaxial, fibra óptica, cable de par trenzado de cobre
  - 10base-2, 10base-T, 10base-F
- Longitud máxima de trama: 1500 bytes de carga útil + encabezados
- Longitud mínima de trama: 64 bytes.
- Distancia máxima entre estaciones: 2500 metros
  - Con repetidores
- Ante una colisión, se espera un tiempo aleatorio: Binary Exponential Backoff

Binary exponential Backoff

- Retroceso exponencial binario
- Después de una colisión, ¿cuánto esperar?
  - Poco: si hay muchas estaciones esperando transmitir, alta probabilidad de nueva colisión
  - Mucho: se desperdicia mucho tiempo si hay pocas estaciones queriendo transmitir
- Binary exponential backoff: algoritmo adaptativo
- Después de colisión: Se divide el tiempo en ranuras de 2🔀 (512 bits)
- Inicialmente sortea si esperar k=0 o 1 ranura
- Ante cada colisión: duplico la cantidad de ranuras 0 – 3, 0 - 7, etc.
  - Sortea k entre 0 – 2^m-1
- Espero k*(tiempo de 512 bits)
- Máximo 0-1023
- 16 colisiones => reporto fracaso

Servicio ofrecido

- El servicio ofrecido por 802.3 es:
  - Sin conexión (no hay establecimiento entre transmisor y receptor)
  - No confiable (no se envían reconocimientos positivos ni negativos al transmisor. En caso de error, se descarta “silenciosamente”)
    - Deben encargarse las capas superiores de recuperar errores
  - En IEEE 802 existe la opción de servicio confiable, pero en IP no se utiliza
- El sistema, salvo que se esté trabajando fuera de las especificaciones de los cables, conectores, transmisores, receptores, etc., está diseñada para tener una tasa de errores muy baja (del orden de 10^{-10} – 10^{-13})

Formato de trama 802.3

Preámbulo	Marca Inicio	Dir. destino	Dir. Origen	Tipo	Datos	Relleno	CRC
7	1	6	6	2	0-1500	0-46	4

bytes

- Preámbulo: secuencia de bits para sincronizar receptor con transmisor
  - 10101010 en la 802.3 original
- Marca de inicio: byte que indica el comienzo de la trama (10101011)
- Direcciones origen y destino: direcciones de capa MAC (6 bytes cada una)
- Tipo: Indica el protocolo de capa superior (IP, IPv6, ARP, etc)
- Datos: los datos a enviar, proveniente de las capas superiores
- Relleno: se usa en caso que los datos sean pocos y no lleguemos al largo mínimo de trama
- CRC: Código de redundancia cíclica para detección de errores
- El formato de trama se mantiene en las distintas versiones de 802.3
  - Opción de aumentar el tamaño del campo de datos: Jumbo frames

Evolución de 802.3. Links y capa física

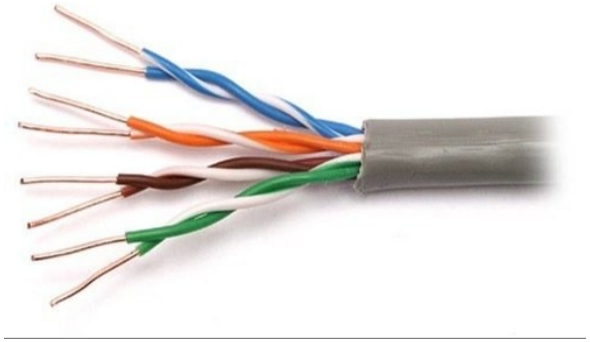
- “Fast Ethernet” (1995) IEEE 802.3u. 100 Mbps sobre cable de pares de cobre y sobre fibra
  - Sigue permitiéndose CSMA/CD, repetidores
  - Distancia máxima 100 metros al repetidor, máximo 1 repetidor
- Gigabit Ethernet (1998) IEEE 802.3z, 802.3ab. 1000 Mbps sobre fibra y cable de pares de cobre
  - Sigue permitiéndose CSMA/CD, repetidores
  - En la realidad, solo se utilizan switches
- 10 Gigabit Ethernet (2003-2006). Fibra y cable de pares de cobre
  - Ya no se permite CSMA/CD
- 40 Gbps y 100 Gbps (2010+) 802.3ba. Fibra y cables de cobre (armados)
- 25 Gbps
- La capa MAC varía muy poco (a velocidades por encima de 1 Gbps no se permite CSMA/CD), el formato de trama tampoco varía
- La capa física es completamente distinta.
- ¿Es la misma red? ….

Half duplex versus Full Duplex

- Se introdujeron dispositivos que procesan las tramas en capa 2 (switches)
- Una vez que tengo un canal para transmisión y otro para recepción independientes, ya no es necesario utilizar CSMA/CD ya que no hay posibilidad de colisiones
- Podemos transmitir y recibir simultáneamente
- Se definió la posibilidad de transmitir en full duplex
- También se definieron mensajes para poder negociar el modo de funcionamiento (half/full duplex, velocidad)
- Por encima de 1 Gbps, solo está permitido el funcionamiento full duplex

Medios físicos en Ethernet

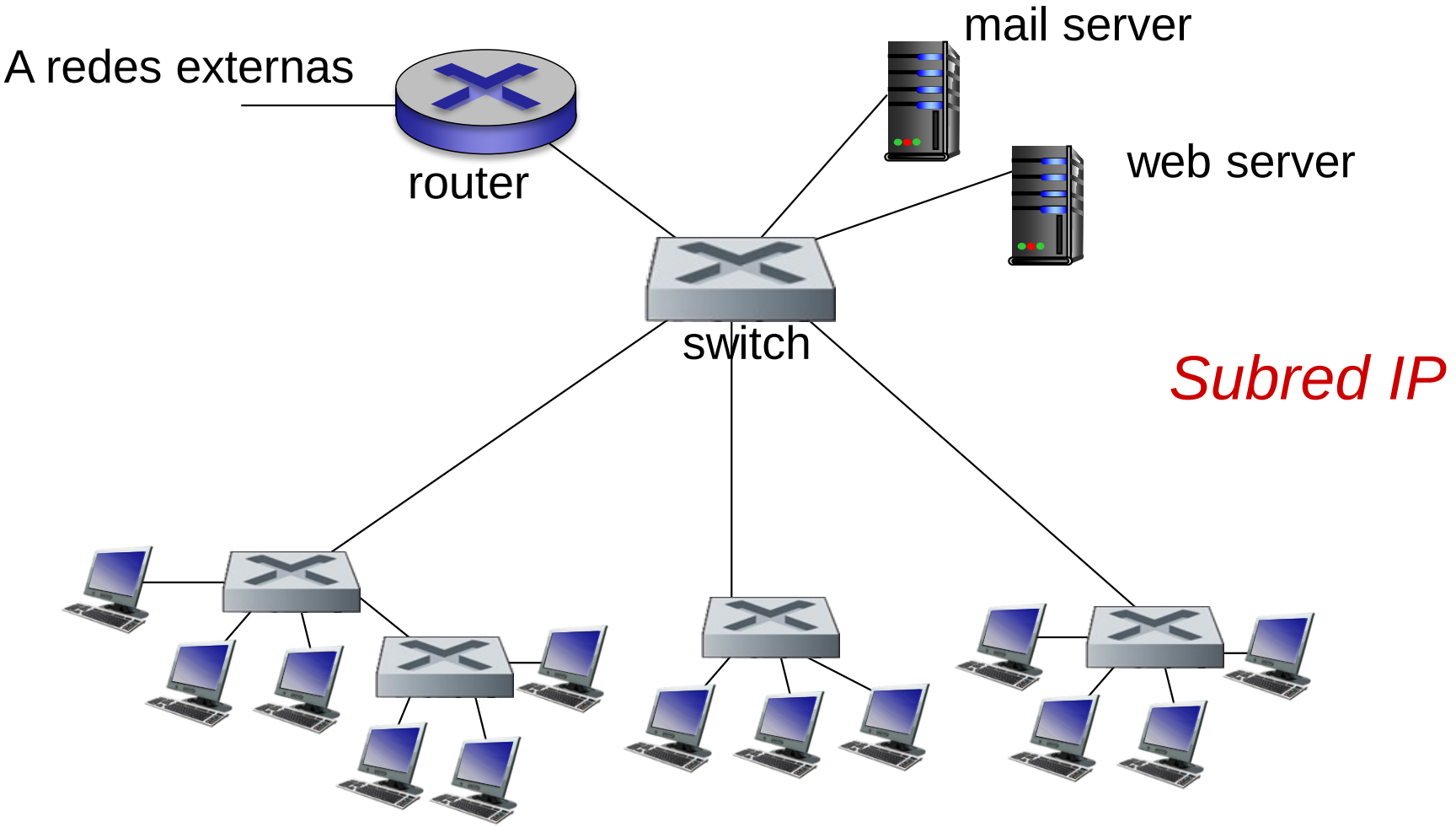
- Cable coaxial: solo en 802.3 a 10 Mbps (obsoleto)
- Par trenzado: 4 pares de alambres de cobre
  - Categoría 3: 10 Mbps
  - Categoría 5: 100 Mbps
  - Categoría 5e, 6: 1 Gbps
  - Categoría 7, 8: 10 Gbps (cables armados)
- Otros cables de cobre armados: 40 Gbps
- Fibra óptica: todas las velocidades
  - Multimodo (OM3, OM4): cortas distancias. Dependiendo de la velocidad, entre 1000 y 100 metros
  - Monomodo: mayores distancias. 20, 40, 80 y más



Switches ethernet

- Dispositivo en capa 2
- Realiza store and forward de las tramas
- Verifica la suma de comprobación
- Examina la dirección MAC de destino, y realiza un reenvío selectivo a uno o más puertos de salida
- En segmentos con colisiones, implementa CSMA/CD
- En segmentos con un solo equipo, puede funcionar en modo full-duplex
  - Es el funcionamiento habitual hoy en día
- Es transparente. Los equipos conectados no notan la presencia de un switch
- Son “plug and play”. No requieren configuración, aprenden de forma transparente

Ejemplo de red con switches

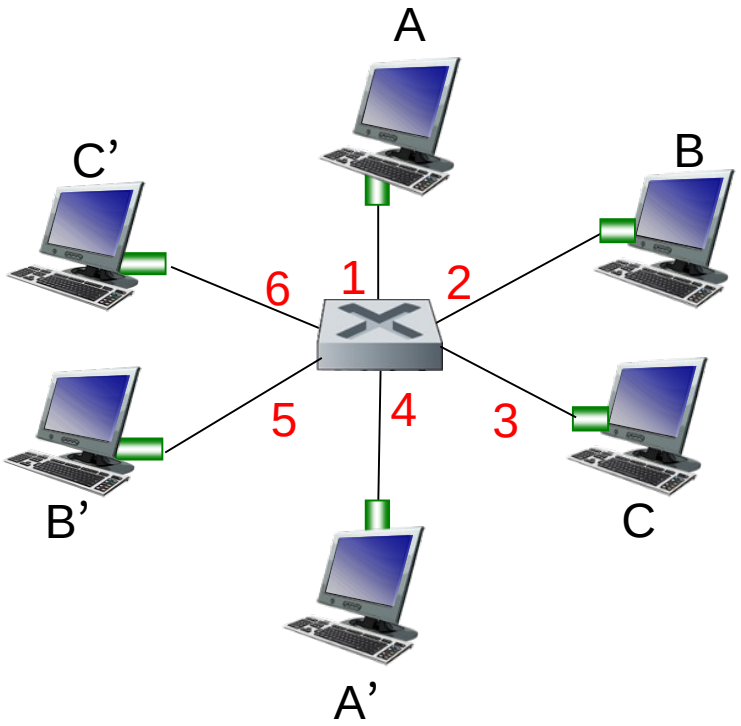


Funcionamiento de un switch

- El equipo dispone de múltiples puertos Ethernet (802.3), en muchos casos distintas variantes (velocidad, medio físico….)
  - Puede tener cientos de puertos
- Funciona en modo “store and forward”. Lee cada trama entrante, verifica la suma de comprobación, y de no haber problemas la copia a uno o más puertos de salida
- Dado que múltiples tramas pueden ir destinadas al mismo puerto de salida, habrá buffers para almacenar las tramas
- Cada puerto define su propio segmento. Las colisiones no se “propagan” dentro del switch
- Si las conexiones son punto a punto (de una máquina a un switch o de un switch a otro), podemos trabajar en full-duplex
  - No es necesario CSMA/CD
  - No hay colisiones!!!

Switch: múltiples transmisiones simultáneas

- Como cada host tiene una conexión directa con el switch, pueden estar varios transmitiendo al mismo tiempo
- Por ejemplo, en la figura A puede transmitir a A’ al mismo tiempo que B transmite a B’
  - Y B’ podría a su vez estar transmitiendo
- La cantidad de tramas que se pueden procesar simultáneamente depende de la capacidad del switch
- Un switch “full line rate” es capaz de enviar y recibir simultáneamente por todos sus puertos continuamente



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

Switch forwarding: MAC table

- Cuando el switch recibe una trama, debe decidir por qué puerto reenviarla
  - Lo hará en función de la dirección MAC de destino de la trama
- Para decidir en qué puerto se encuentra cada dirección MAC, el switch tiene una tabla que relaciona cada dirección MAC con un puerto
- Cada entrada en la tabla tendrá: Dirección MAC, puerto, y tiempo de vida de la entrada
  - El tiempo de vida es para borrar las entradas inactivas de la tabla

Dirección MAC	Puerto	Tiempo
62:FE:F7:11:89:A3	3	9:32
7C:BA:11:E1:55:A1	4	2:40
…..	...	…..

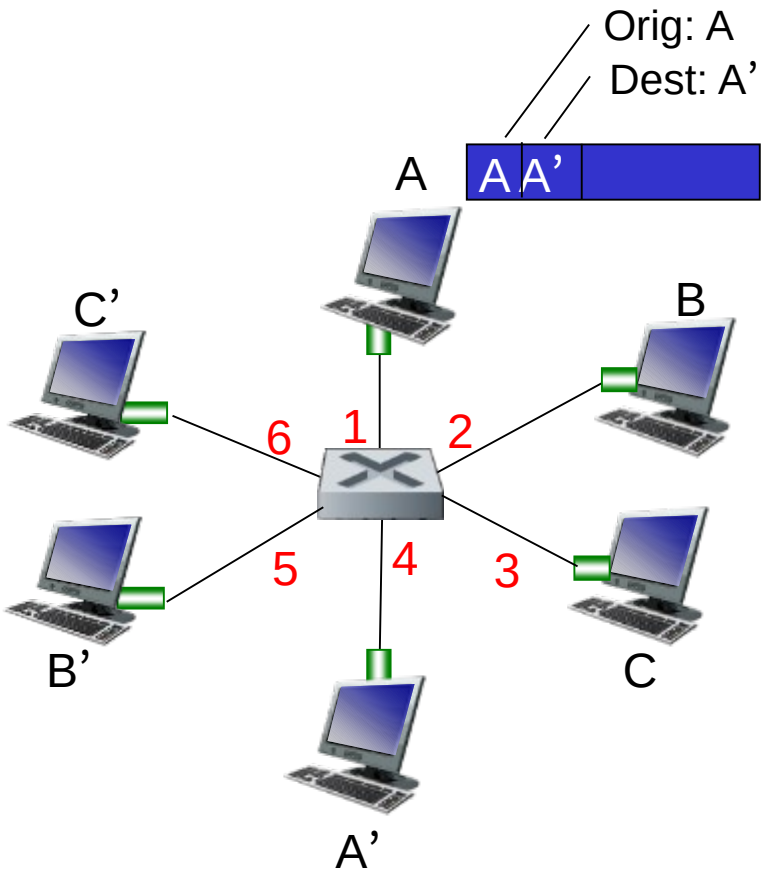
- Direcciones Broadcast: Se reenvía por todos los puertos
- Direcciones desconocidas: Se reenvía por todos los puertos
- Multicast: tratamiento depende del switch (por defecto se inunda)

Auto aprendizaje

- No queremos tener que configurar la tabla: auto aprendizaje
- ¿Cómo podemos aprender dónde está cada dirección MAC?

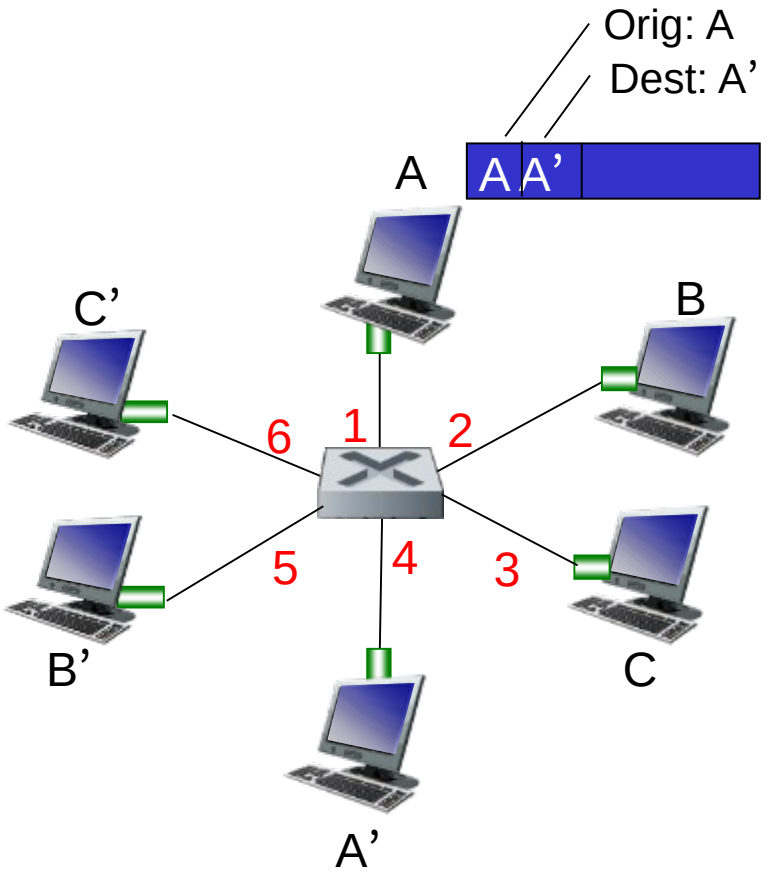
Auto aprendizaje

- No queremos tener que configurar la tabla: auto aprendizaje
- ¿Cómo podemos aprender dónde está cada dirección MAC?



Auto aprendizaje

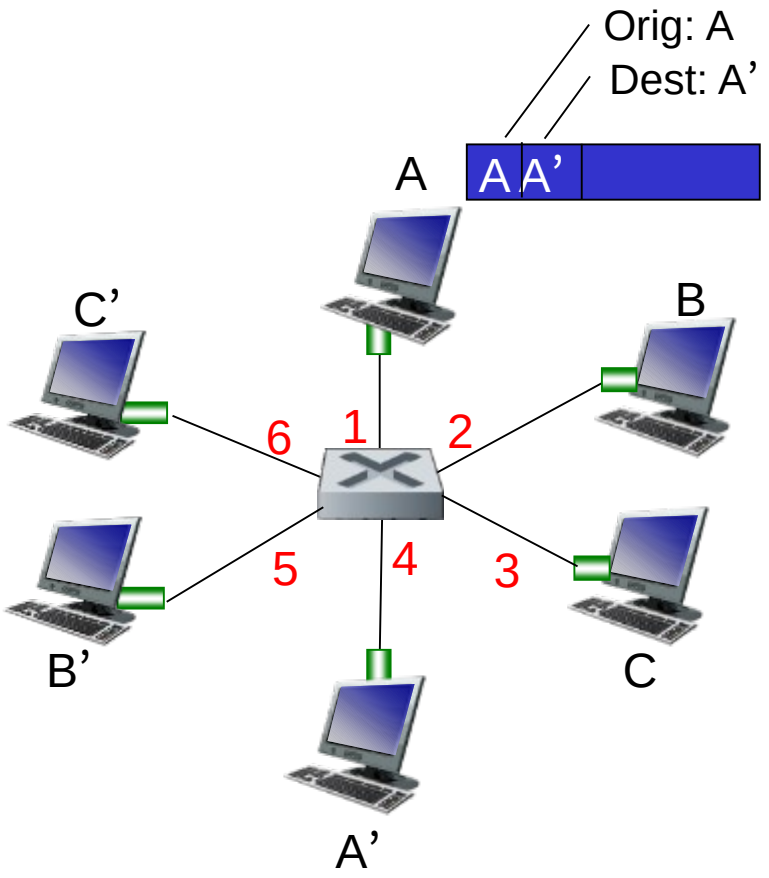
- No queremos tener que configurar la tabla: auto aprendizaje
- ¿Cómo podemos aprender dónde está cada dirección MAC?
- Cuando A envía una trama a A’
  - switch recibe trama
  - Observa dirección DE ORIGEN (A)
  - Agrega entrada en tabla para A



Auto aprendizaje

- No queremos tener que configurar la tabla: auto aprendizaje
- ¿Cómo podemos aprender dónde está cada dirección MAC?
- Cuando A envía una trama a A’
  - switch recibe trama
  - Observa dirección DE ORIGEN (A)
  - Agrega entrada en tabla para A

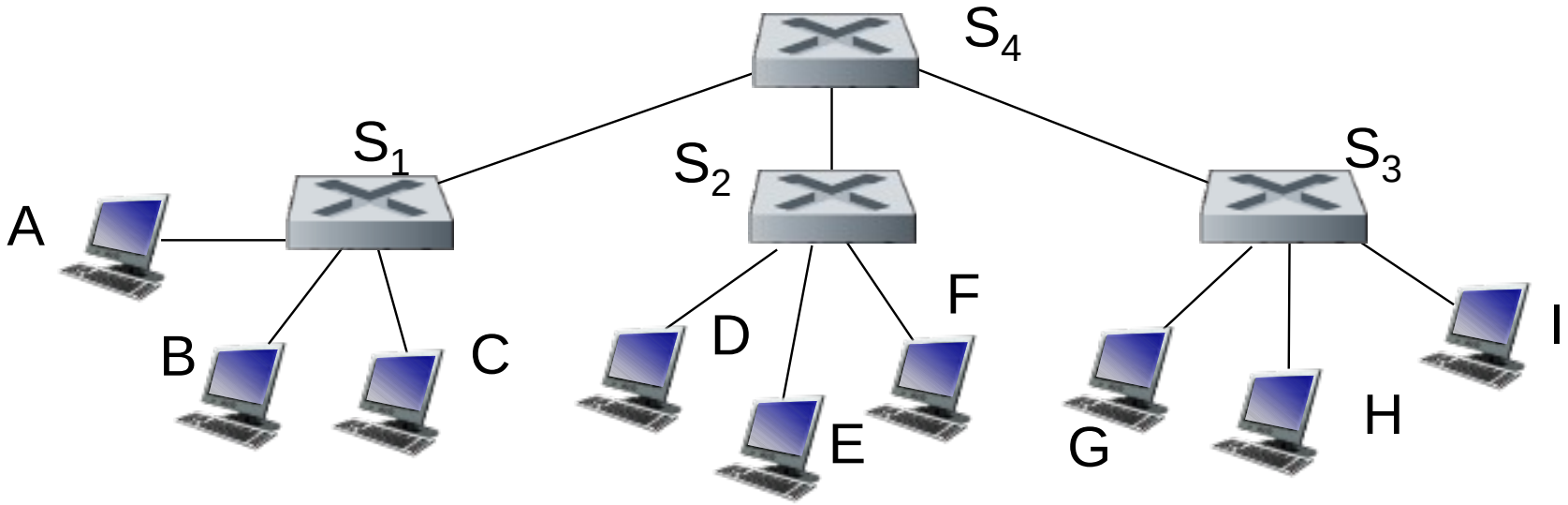
Dirección MAC	Puerto	TTL
A	1	20:00
...	...	...



Filtrado y forwarding

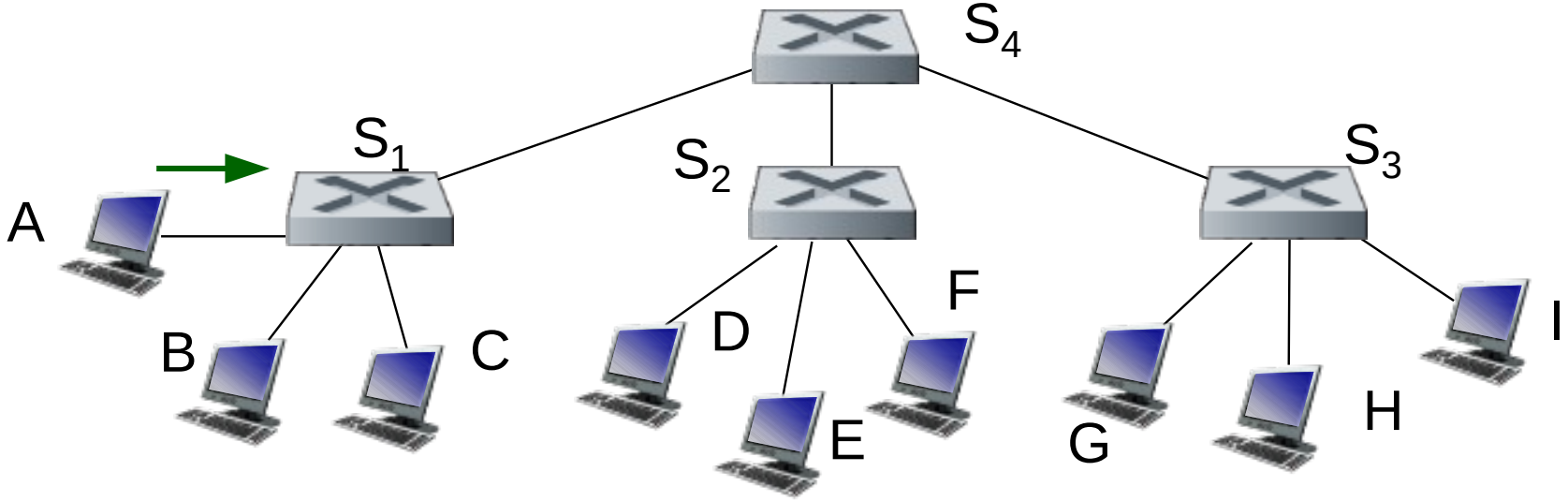
- Cuando el switch recibe una trama:
  1) Guardar o actualizar entrada para la dirección MAC de origen
  2) Si dirección de destino es broadcast → Inundar
  3) Buscar dirección de destino en la tabla
  4) Si no se encontró en la tabla → Inundar
  5) Si se encontró en la tabla:
     - Si el destino está en el mismo segmento por el que ingresó la trama, descartar
     - De lo contrario enviar por el puerto correspondiente

Ejemplo



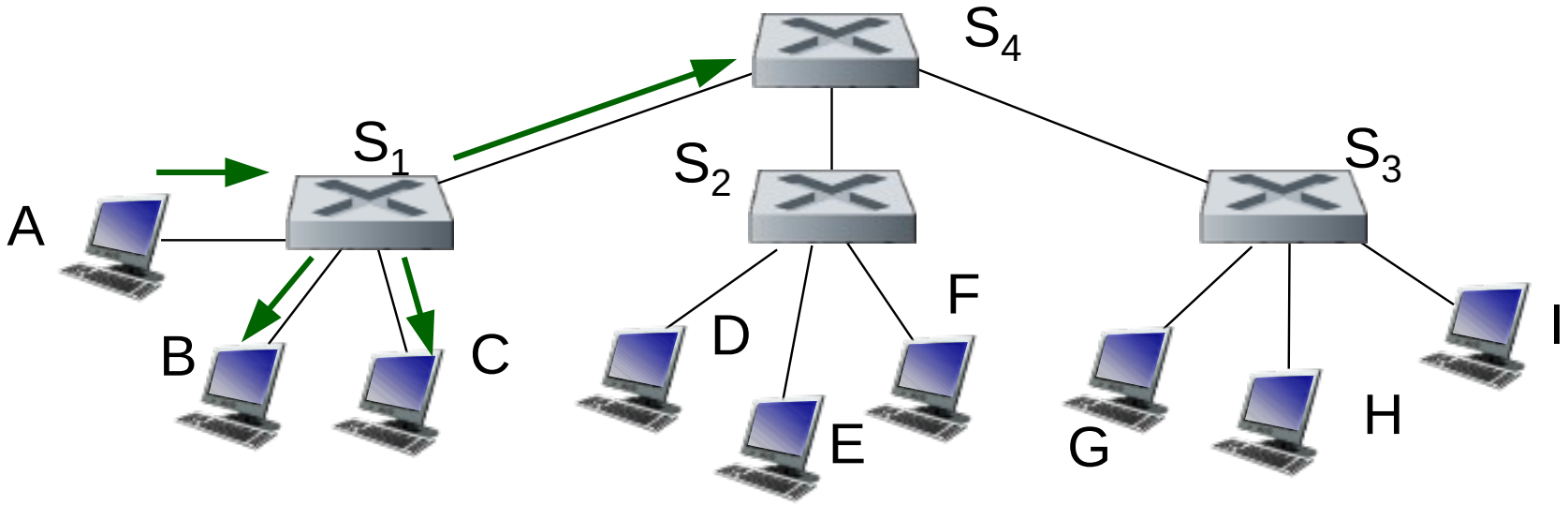
- Tablas inicialmente vacías

Ejemplo



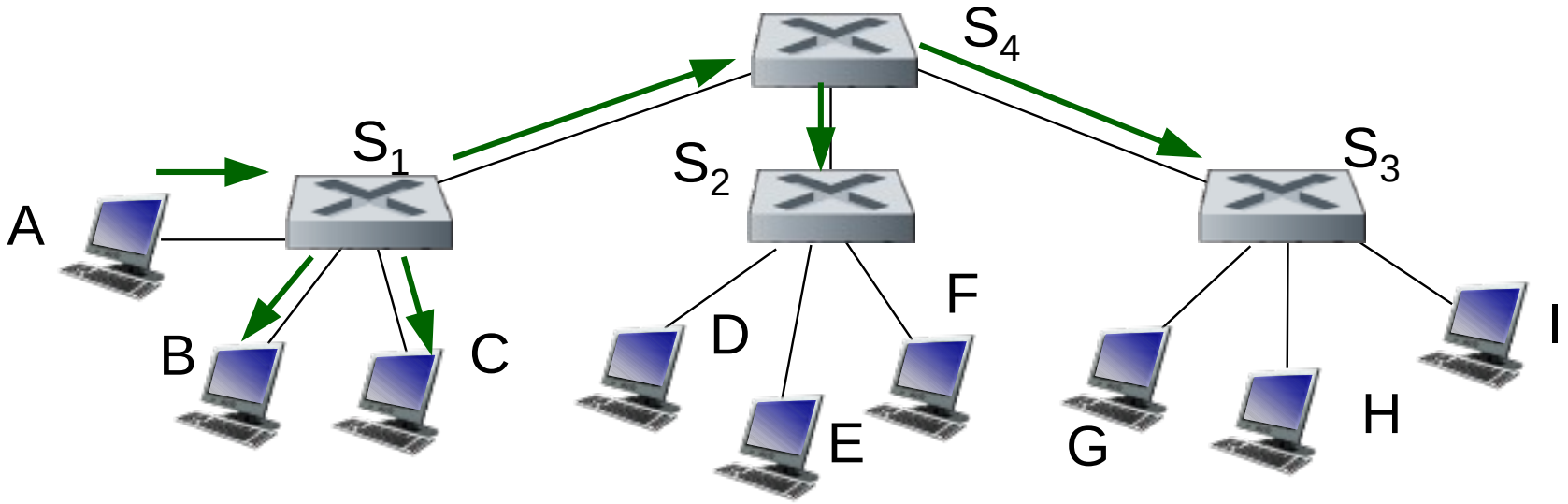
- A envía trama a B:

Ejemplo



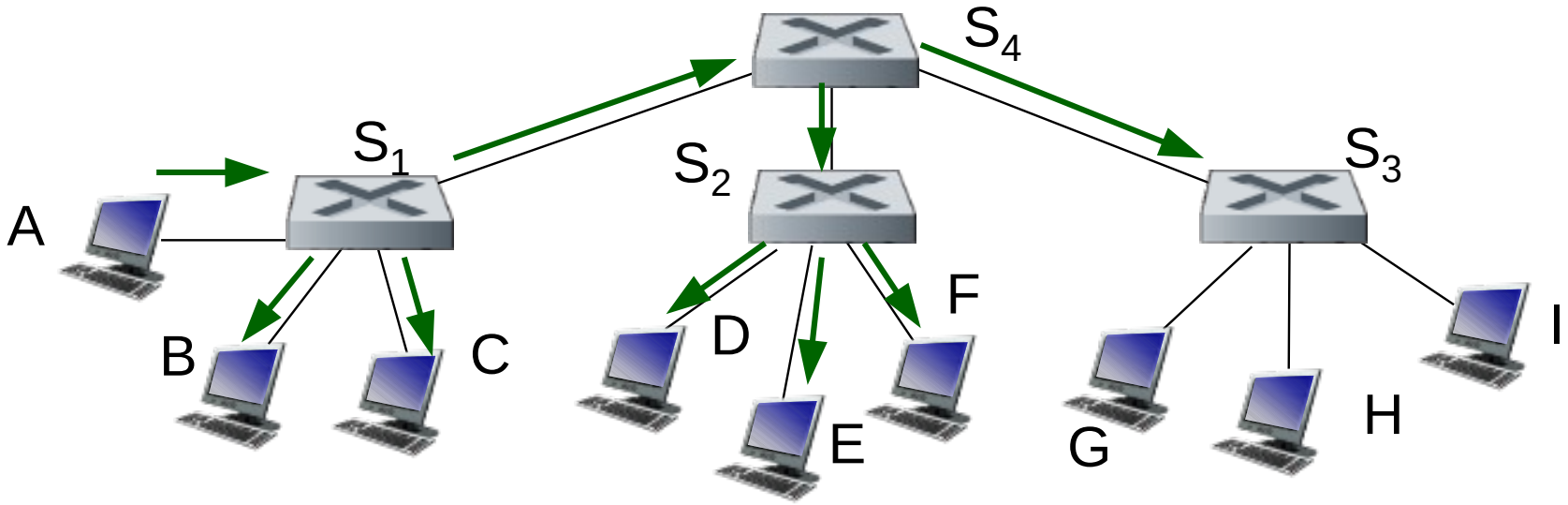
- A envía trama a B:
  - S1 no sabe dónde está B, envía trama a B, C y S4
    - Aprende dónde está A

Ejemplo



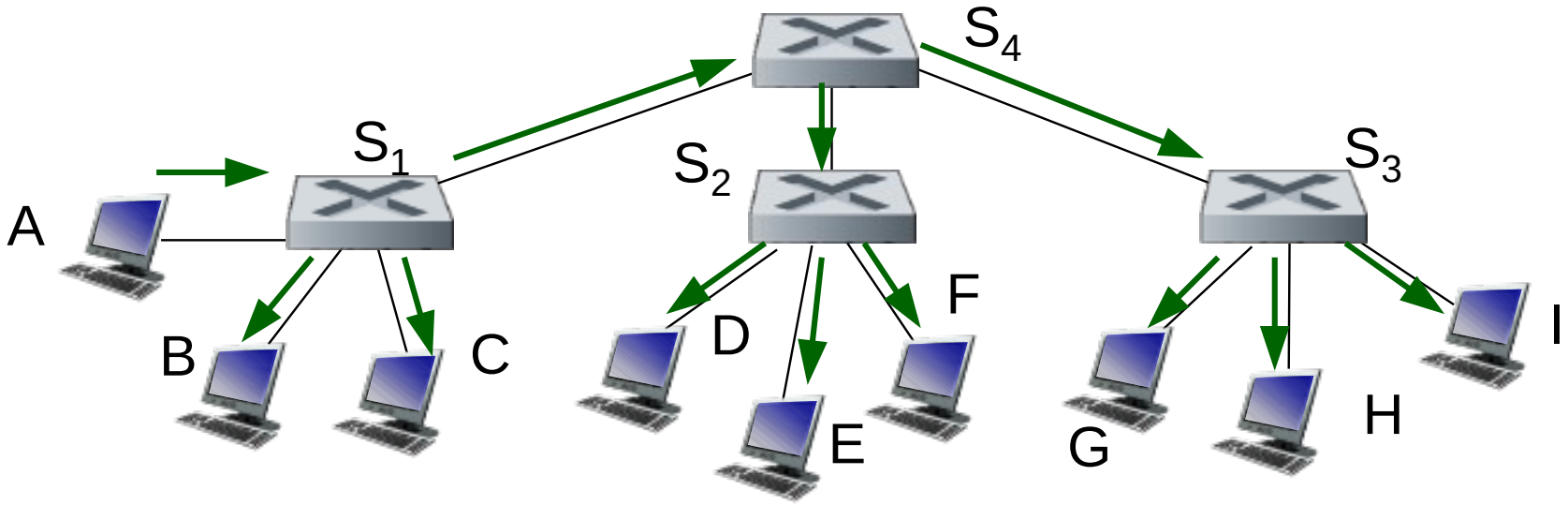
- A envía trama a B:
  - S1 no sabe dónde está B, envía trama a B, C y S4
    - Aprende dónde está A
  - S4 no sabe dónde está B. Envía a S2 y S3
    - Aprende dónde está A

Ejemplo



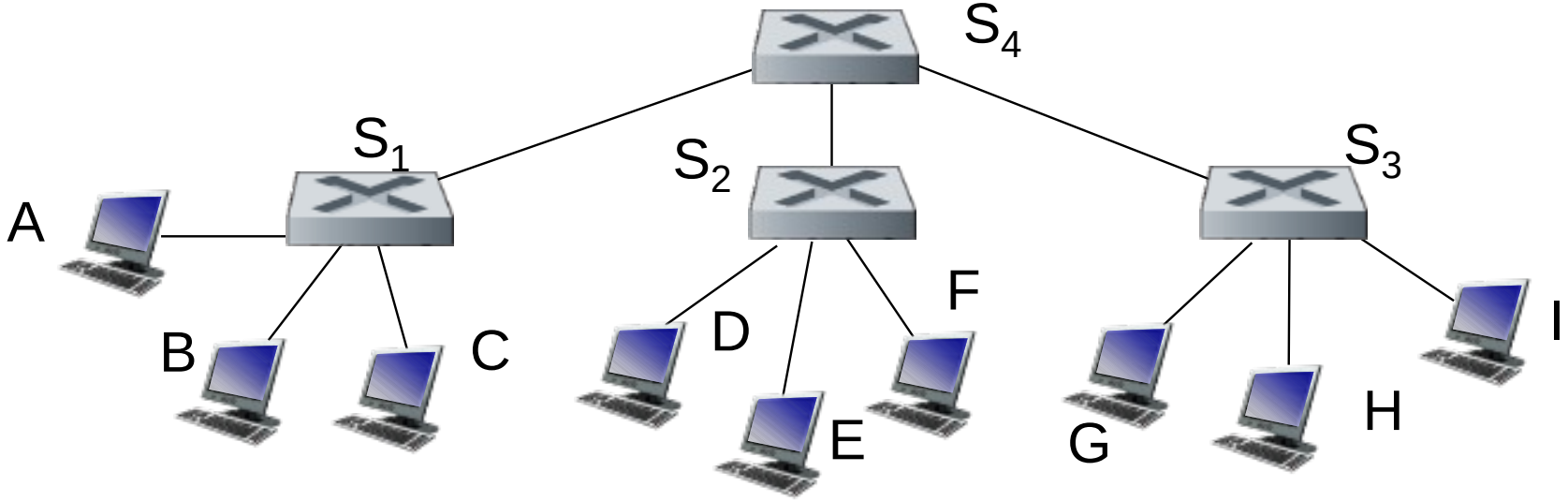
- A envía trama a B:
  - S1 no sabe dónde está B, envía trama a B, C y S4
    - Aprende dónde está A
  - S4 no sabe dónde está B. Envía a S2 y S3
    - Aprende dónde está A
  - S2 no sabe dónde está B, envía a D, E, F
    - Aprende dónde está A

Ejemplo

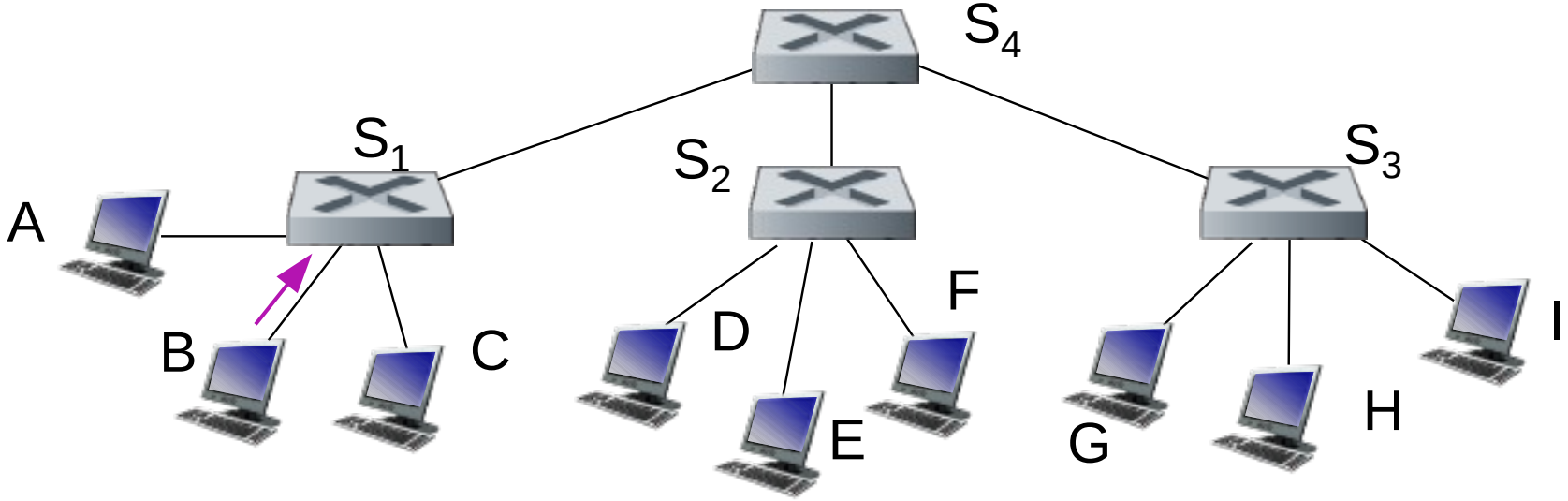


- A envía trama a B:
  - S1 no sabe dónde está B, envía trama a B, C y S4
    - Aprende dónde está A
  - S4 no sabe dónde está B. Envía a S2 y S3
    - Aprende dónde está A
  - S2 no sabe dónde está B, envía a D, E, F
    - Aprende dónde está A
  - S3 no sabe dónde está B, envía a G, H, I
    - Aprende dónde está A

Ejemplo

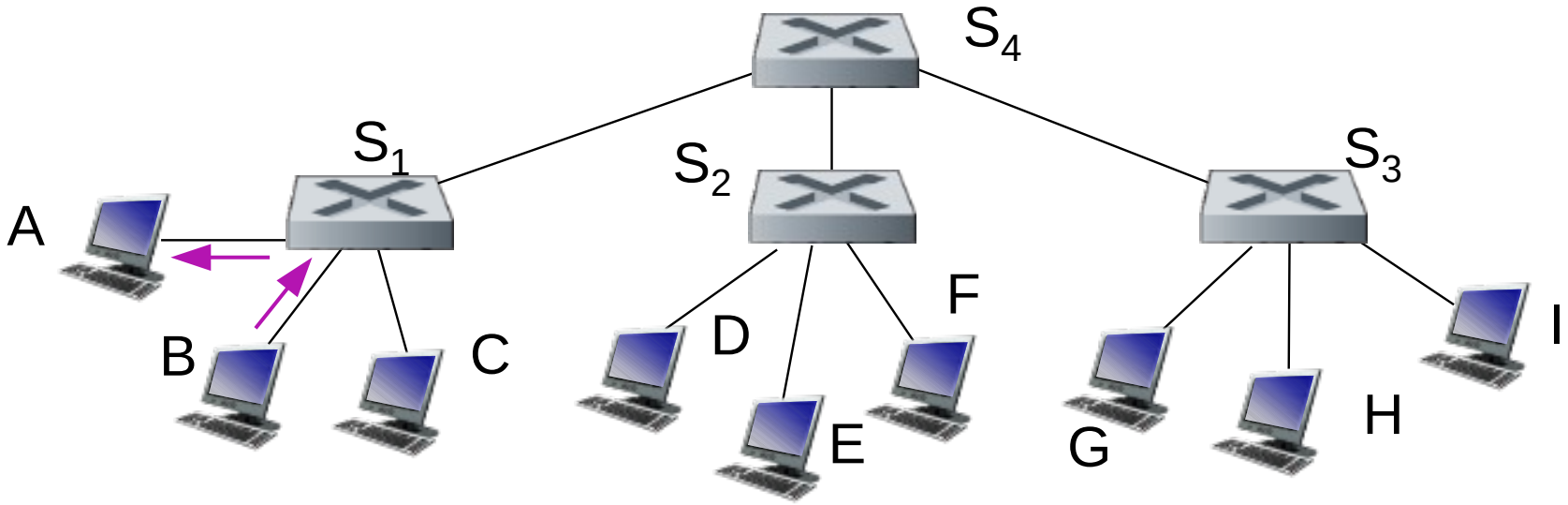


Ejemplo



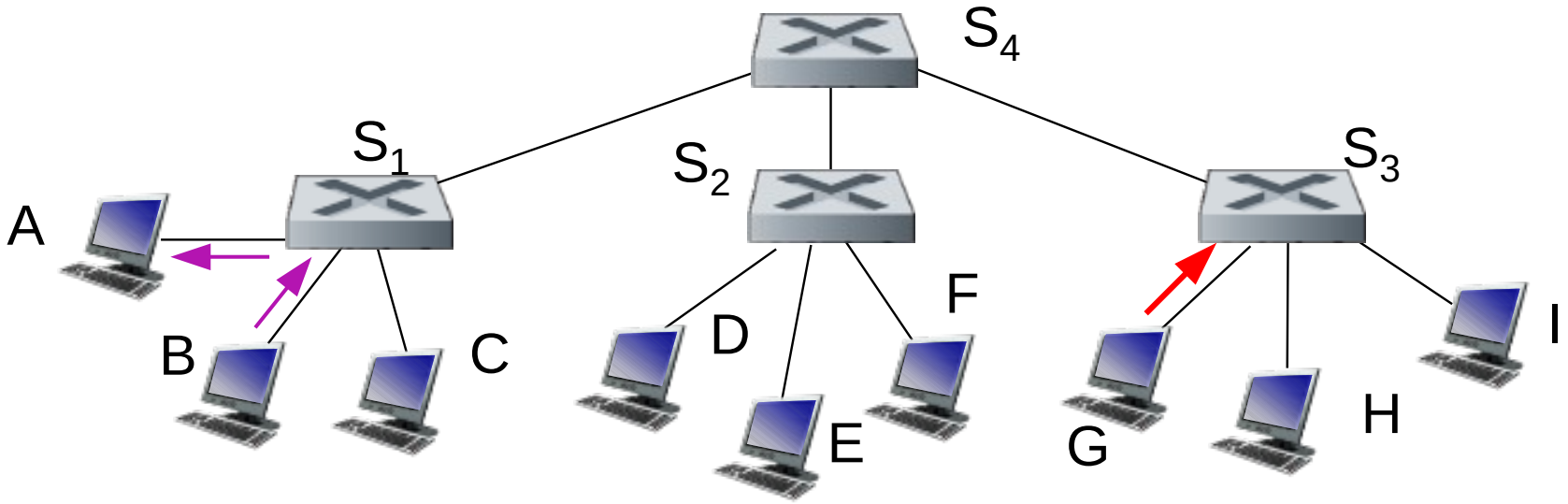
- B envía trama a A:

Ejemplo



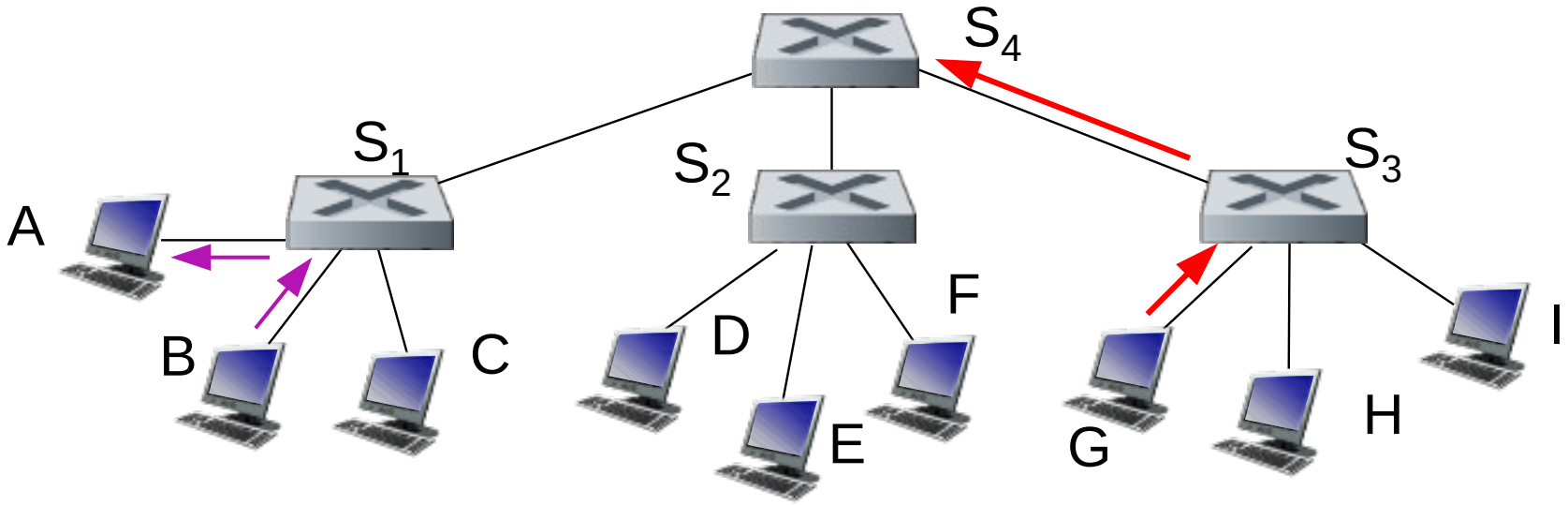
- B envía trama a A:
  - S1 sabe dónde está A, solo le envía a A
    - Aprende dónde está B

Ejemplo



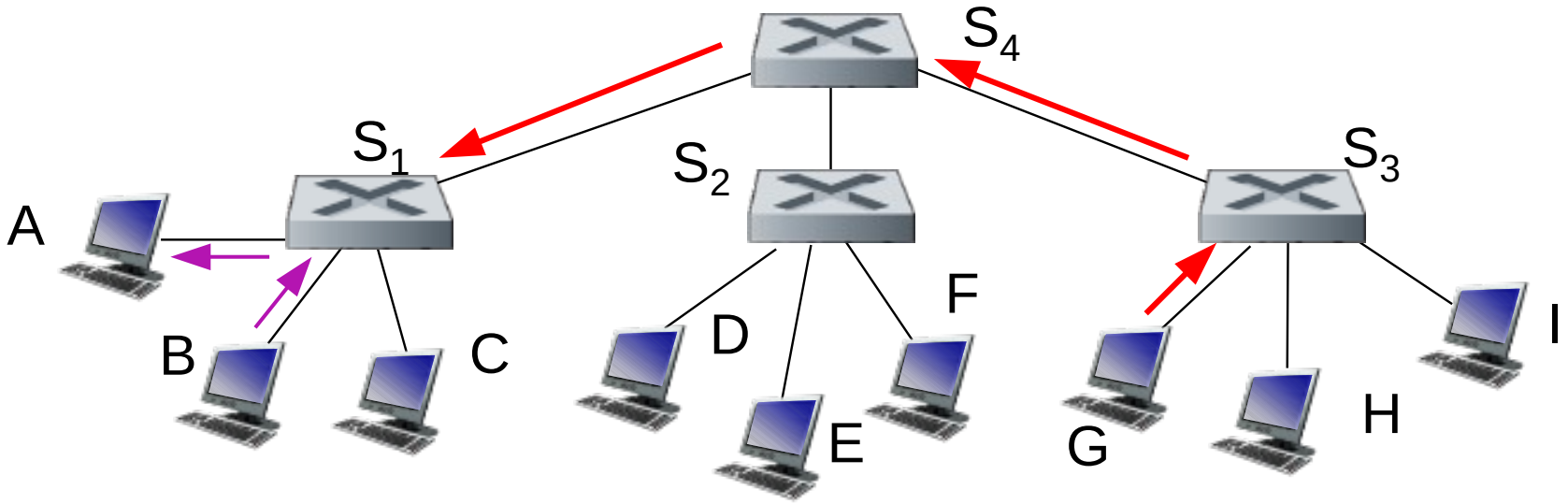
- B envía trama a A:
  - S1 sabe dónde está A, solo le envía a A
    - Aprende dónde está B
- G envía trama a A

Ejemplo



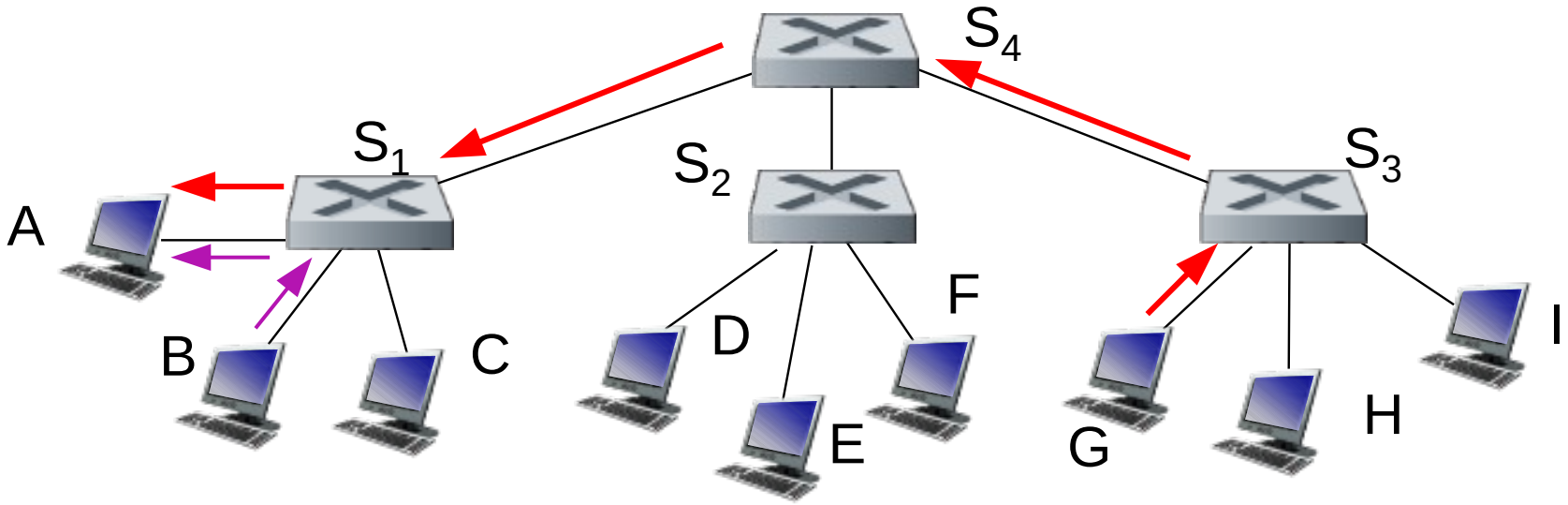
- B envía trama a A:
  - S1 sabe dónde está A, solo le envía a A
    - Aprende dónde está B
- G envía trama a A
  - S3 envía trama a S4
    - Aprende dónde está G

Ejemplo



- B envía trama a A:
  - S1 sabe dónde está A, solo le envía a A
    - Aprende dónde está B
- G envía trama a A
  - S3 envía trama a S4
    - Aprende dónde está G
  - S4 envía trama a S1
    - Aprende dónde está G

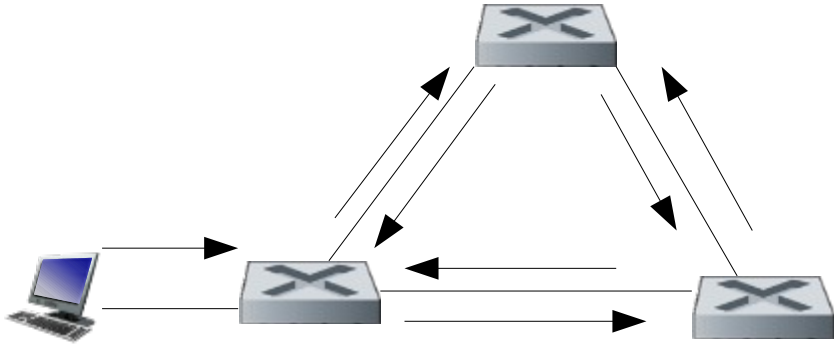
Ejemplo



- B envía trama a A:
  - S1 sabe dónde está A, solo le envía a A
    - Aprende dónde está B
- G envía trama a A
  - S3 envía trama a S4
    - Aprende dónde está G
  - S4 envía trama a S1
    - Aprende dónde está G
  - S1 envía trama a A
    - Aprende dónde está G

Loops en capa 2

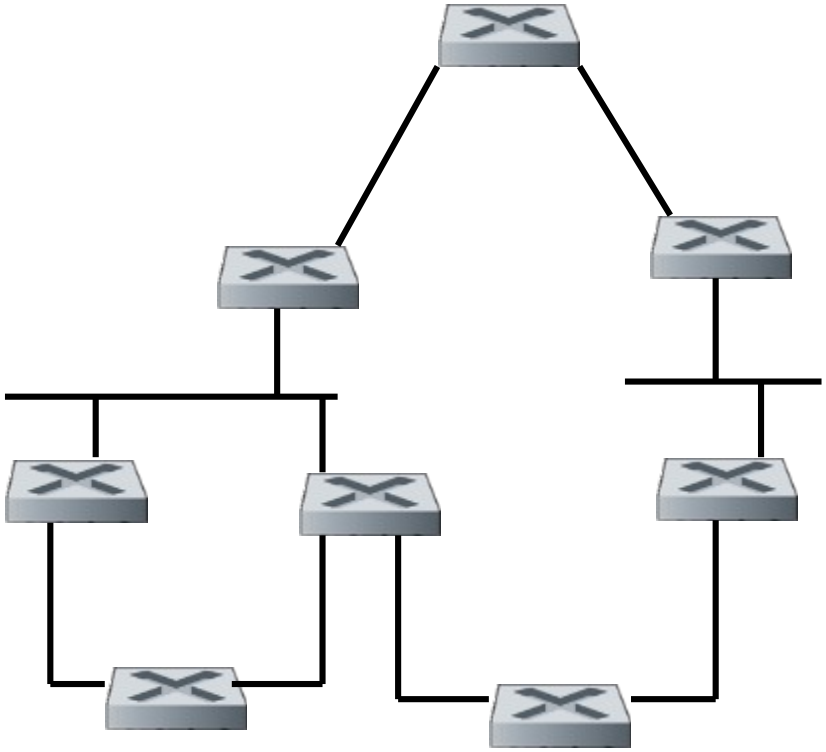
- Loops
  - Por error
  - Porque queremos redundancia
- ¿Qué pasa en Ethernet si se genera un loop?
- Tramas Broadcast
- Tramas para las que no tengo una entrada en la tabla de los switches



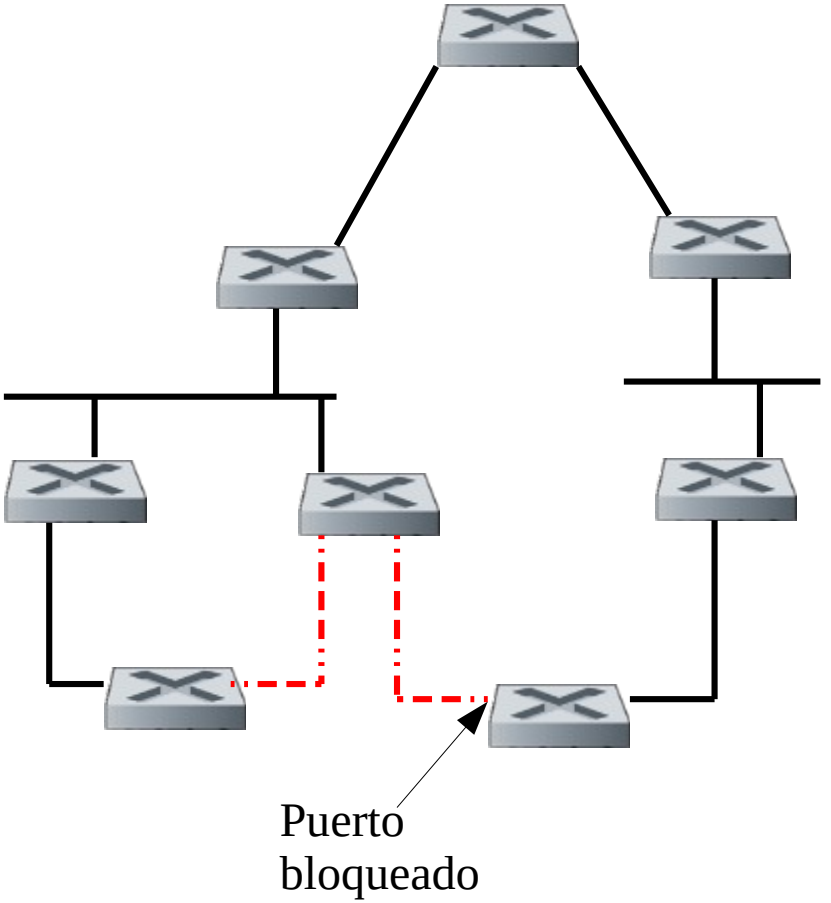
Spanning tree (802.1D)

- Solución tradicional para evitar los loops
- Protocolo de capa de enlace entre switches
- Originalmente 802.1D.
  - Rapid Spanning Tree: 802.1w
  - Multiple Spanning Tree: 802.1s
- Construye un árbol sin loops bloqueando los links redundantes
  - Se elige un puerto como raíz
  - Desde la raiz se van eligiendo links no redundantes para llegar a todos los nodos
  - Los links redundantes se mantienen bloqueados
  - Ante una falla de un link, se desbloquea link redundante

Topología Física



Spanning Tree

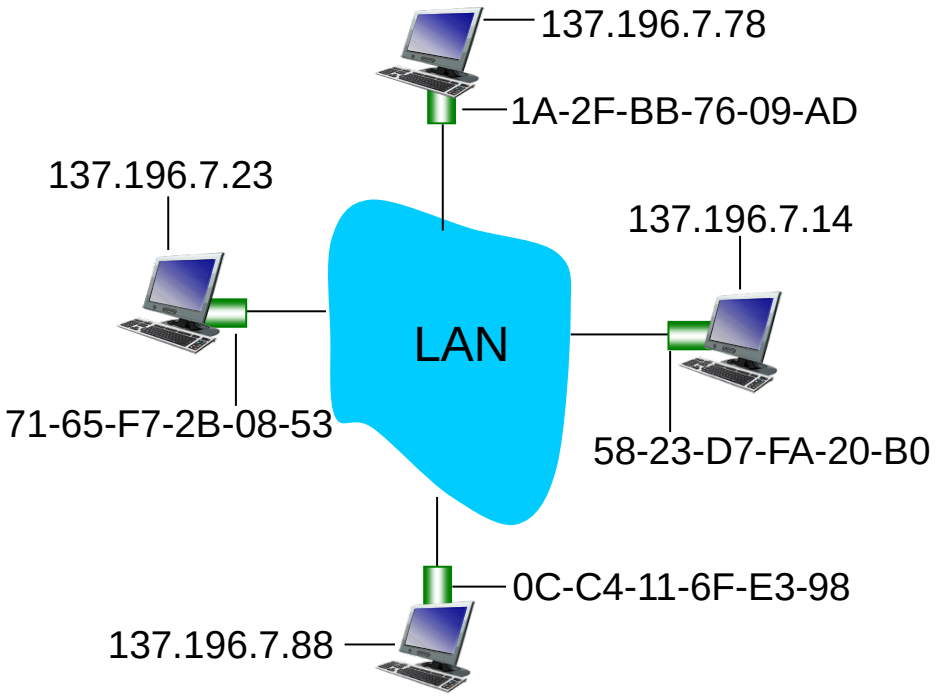


Otras soluciones

- Desventajas de Spanning Tree
  - Convergencia lenta
  - No se pueden utilizar enlaces alternativos
- Alternativas:
  - Utilizar un protocolo de enrutamiento dinámico
    - Ej TRILL (Transparent Interconnection of Lots of Links)
    - Ej SPB (Shortest Path Bridging, 802.1aq)
  - SDN
    - Controlador configura caminos

Relación entre direcciones IP y MAC. ARP

- Cada equipo tendrá una dirección IP (capa 3) y una dirección MAC
- ¿Cómo enviamos un paquete a otro equipo en la LAN, usando la capa MAC?
  - Ejemplo: en la figura, 137.196.7.23 quiere enviar paquete a 137.196.7.78
  - Precisa obtener la dirección MAC correspondiente 1A-2F-BB-76-09-AD
- Se utiliza el protocolo ARP (Address Resolution Protocol)
- Cada máquina tendrá una tabla relacionando la dirección IP con la dirección MAC
- El protocolo ARP llenará dicha tabla
- Lo veremos detalladamente en el laboratorio



ARP

- Las entradas en la tabla ARP tendrán la relación <IP, MAC, tiempo de vida>

IP	MAC	Tiempo
137.196.7.78	1A:2F:BB:76:09:AD	5:53
137.196.7.14	58:23:D7:FA:20:B0	12:11
…..	…..	…..

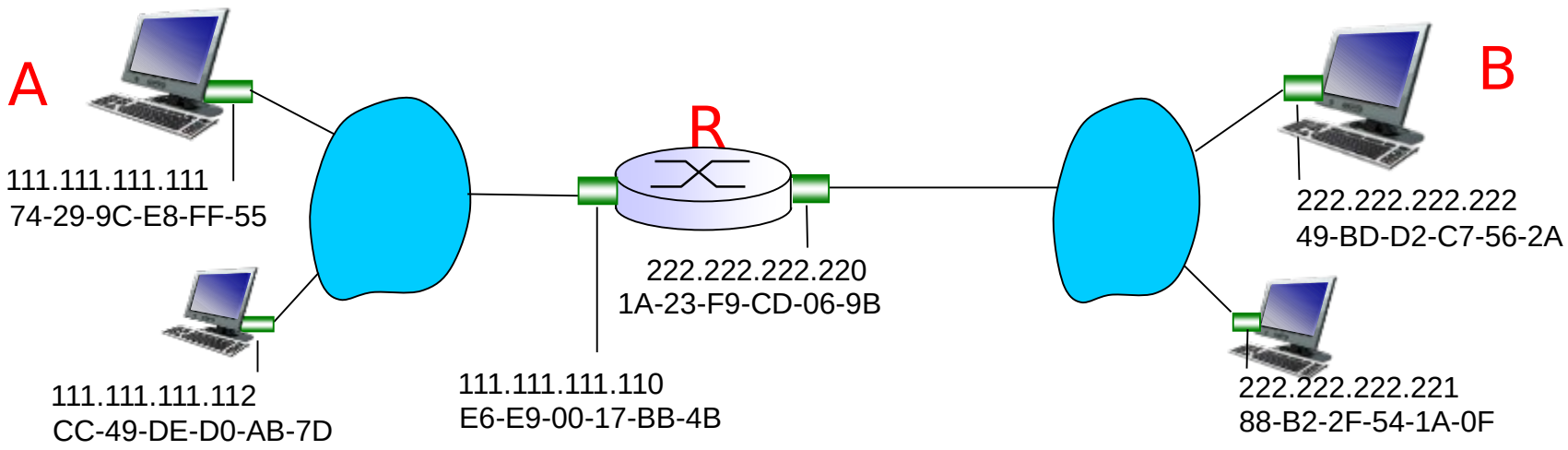
- Solamente tendremos entradas en la tabla para las IPs con las que intercambiamos tráfico
- El tiempo de vida permite borrar las entradas (o refrescarlas si están en uso) luego de un tiempo prudencial (minutos)
- Observar que esta tabla NO está relacionada con la tabla de un switch

Protocolo ARP

- Supongamos que A y B están en la misma LAN. A quiere enviar un paquete a B, pero no tiene una entrada relacionando la IP de B con su MAC
- A envía una trama, con un pedido ARP, con dirección de destino broadcast (FF:FF:FF:FF:FF:FF)
  - Preguntando por la dirección MAC de la IP B
- Todos los nodos de la LAN reciben el pedido.
- B responde
  - B envía una trama a la MAC A con la respuesta (relación IP-B – MAC-B)
- A guarda la relación IP-B – MAC-B en caché por un tiempo de vida (típicamente 20 minutos)
- B también aprende la relación IP-A – MAC-A de la consulta y lo guarda

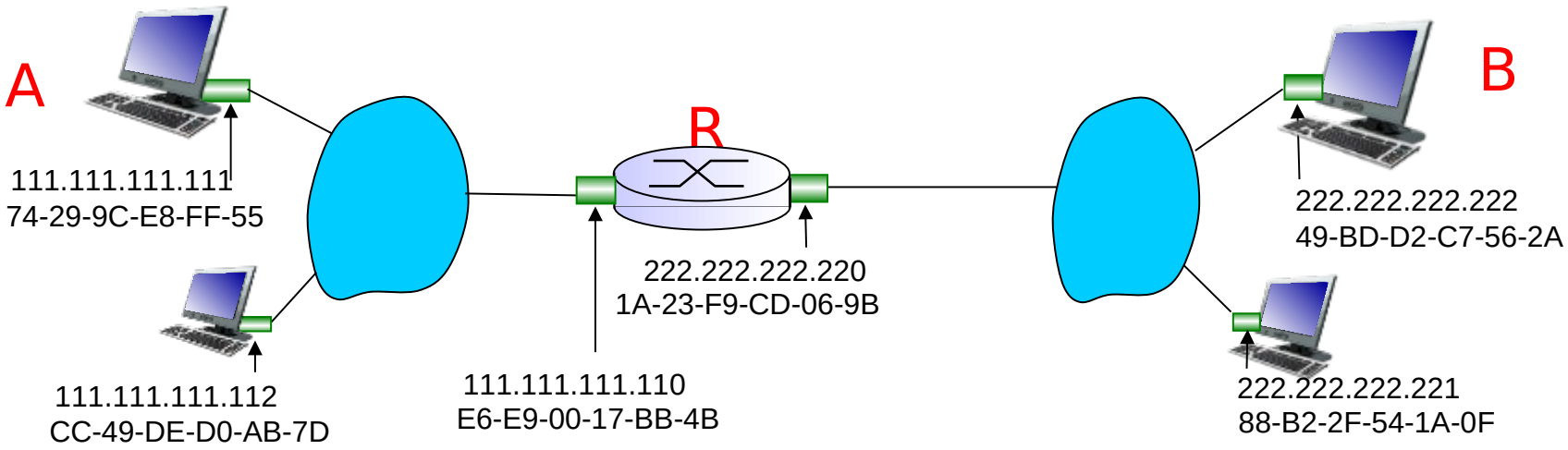
Ejemplo: enrutamiento hacia otra LAN

- A envía un paquete a B (conoce su dirección IP)
  - Su tabla de rutas dice que el próximo salto es 111.111.111.110
  - ¿A quién debe enviarle la trama (capa 2)?
    - A la MAC de R en su LAN
    - Si no la conoce, debe averiguarla utilizando ARP



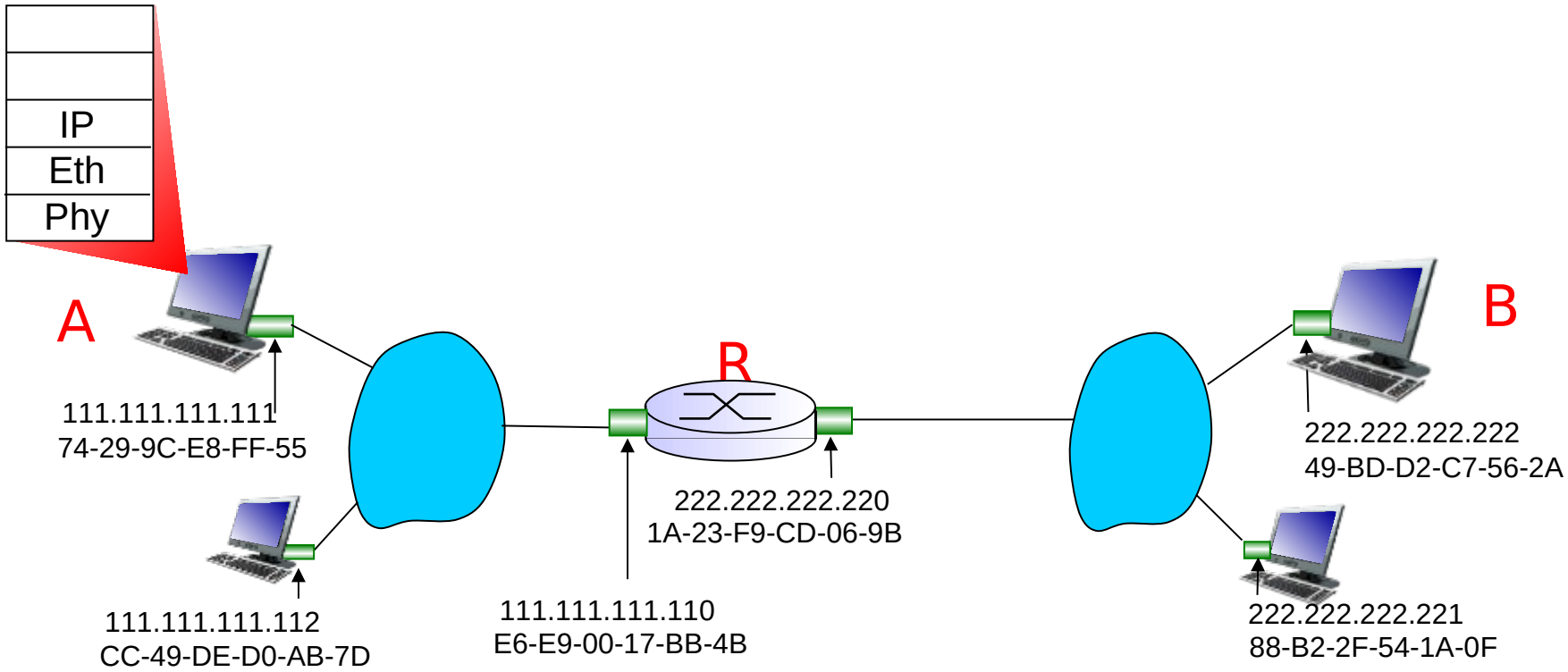
Ejemplo: enrutamiento hacia otra LAN (cont)

- La tabla de rutas dice que el próximo salto es 111.111.111.110.
- Arma el paquete con destino B
- Busca MAC de 111.111.111.110
- Lo envía a la capa de enlace indicando destino E6:E9:00:17:BB:4b



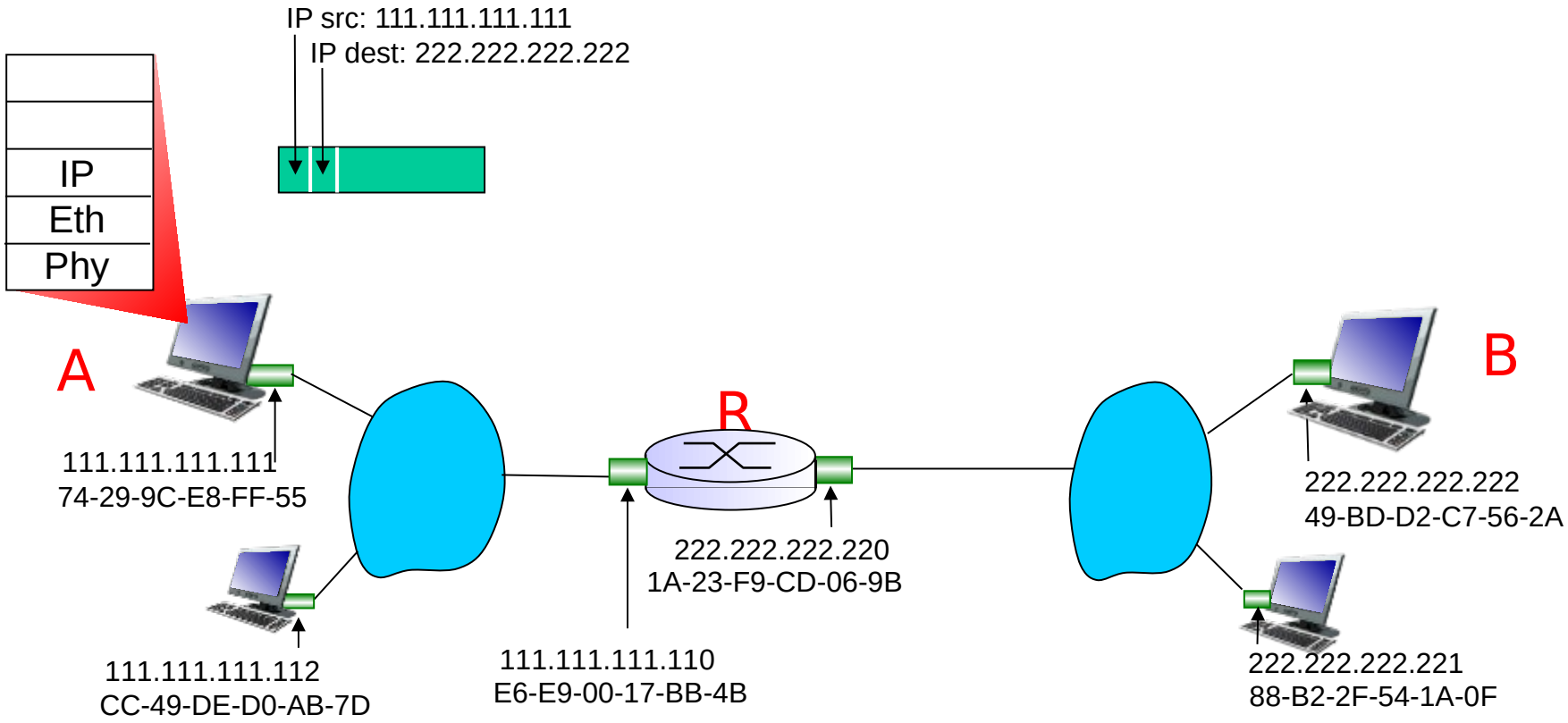
Ejemplo: enrutamiento hacia otra LAN (cont)

- La tabla de rutas dice que el próximo salto es 111.111.111.110.
- Arma el paquete con destino B
- Busca MAC de 111.111.111.110
- Lo envía a la capa de enlace indicando destino E6:E9:00:17:BB:4b



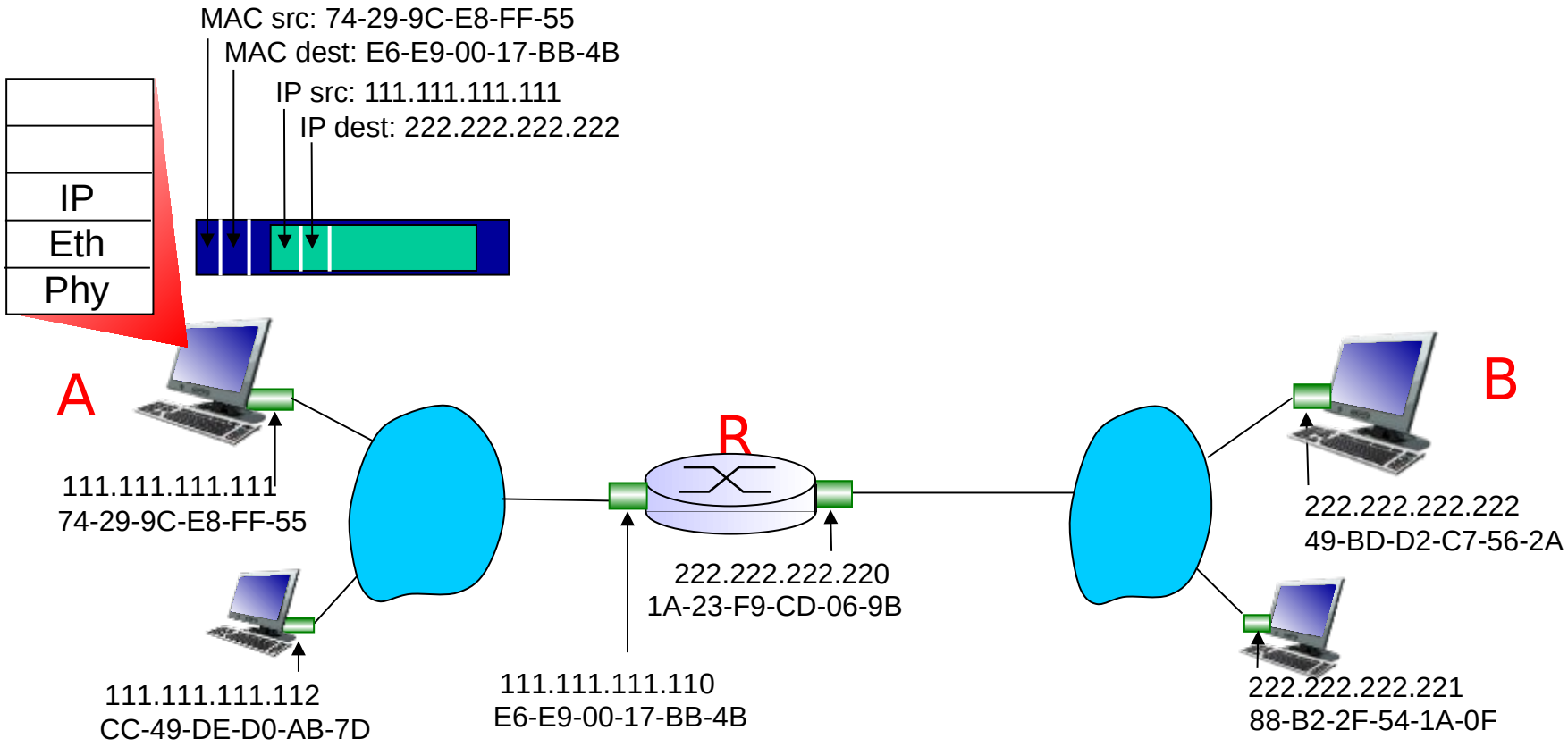
Ejemplo: enrutamiento hacia otra LAN (cont)

- La tabla de rutas dice que el próximo salto es 111.111.111.110.
- Arma el paquete con destino B
- Busca MAC de 111.111.111.110
- Lo envía a la capa de enlace indicando destino E6:E9:00:17:BB:4b



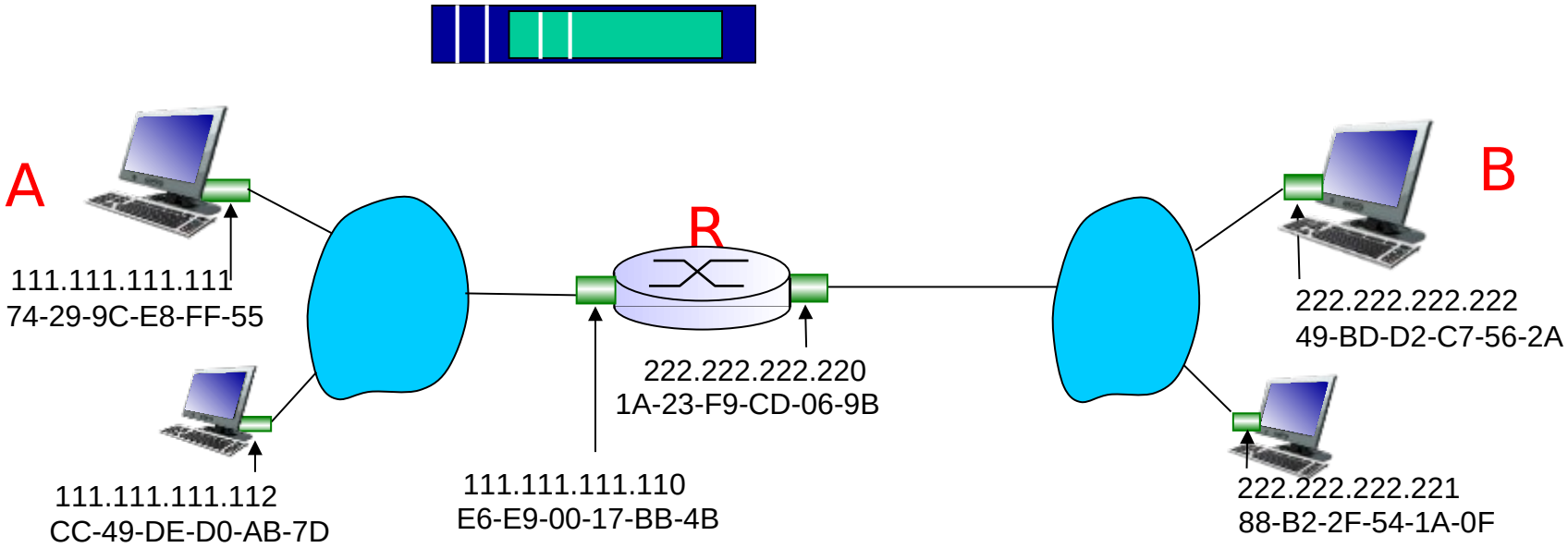
Ejemplo: enrutamiento hacia otra LAN (cont)

- Capa de enlace arma la trama y la envía a la LAN
  - Dirección origen la propia, destino la de R en esa LAN



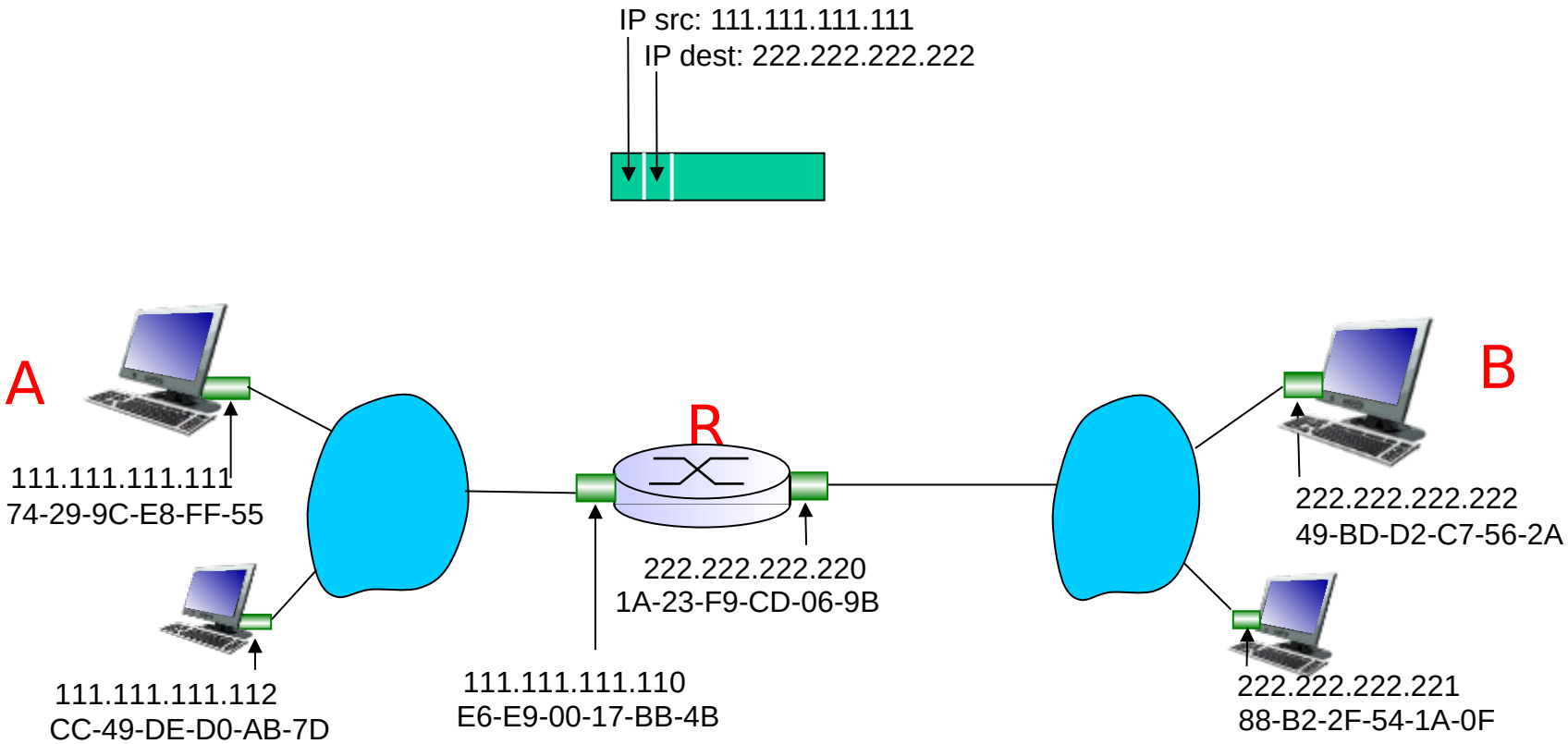
Ejemplo: enrutamiento hacia otra LAN (cont)

- R detecta que en capa MAC está direccionado a el
- Extrae el paquete y lo pasa a capa de red
- Capa de red ve que no es para el y lo enruta



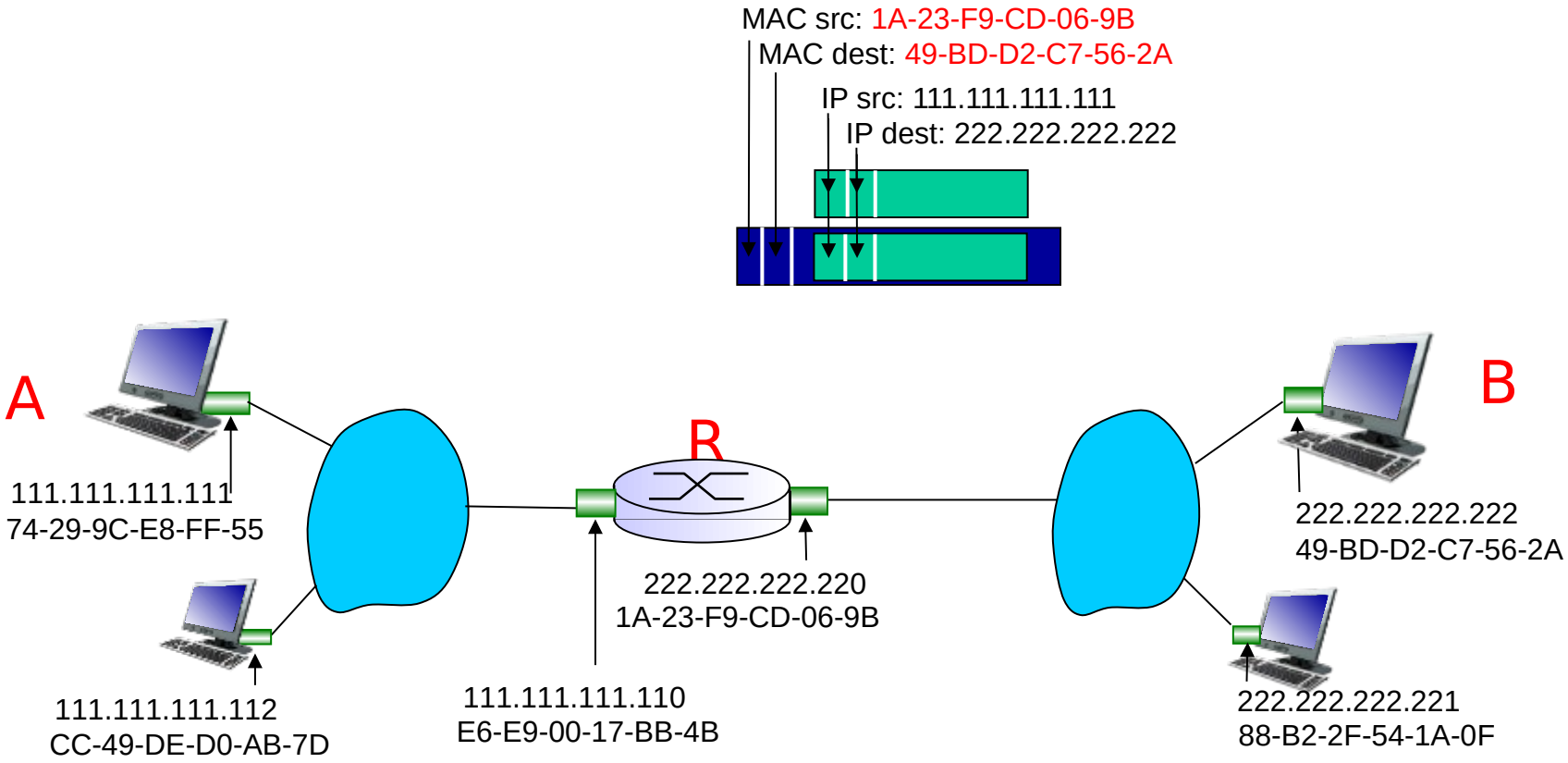
Ejemplo: enrutamiento hacia otra LAN (cont)

- R detecta que en capa MAC está direccionado a el
- Extrae el paquete y lo pasa a capa de red
- Capa de red ve que no es para el y lo enruta



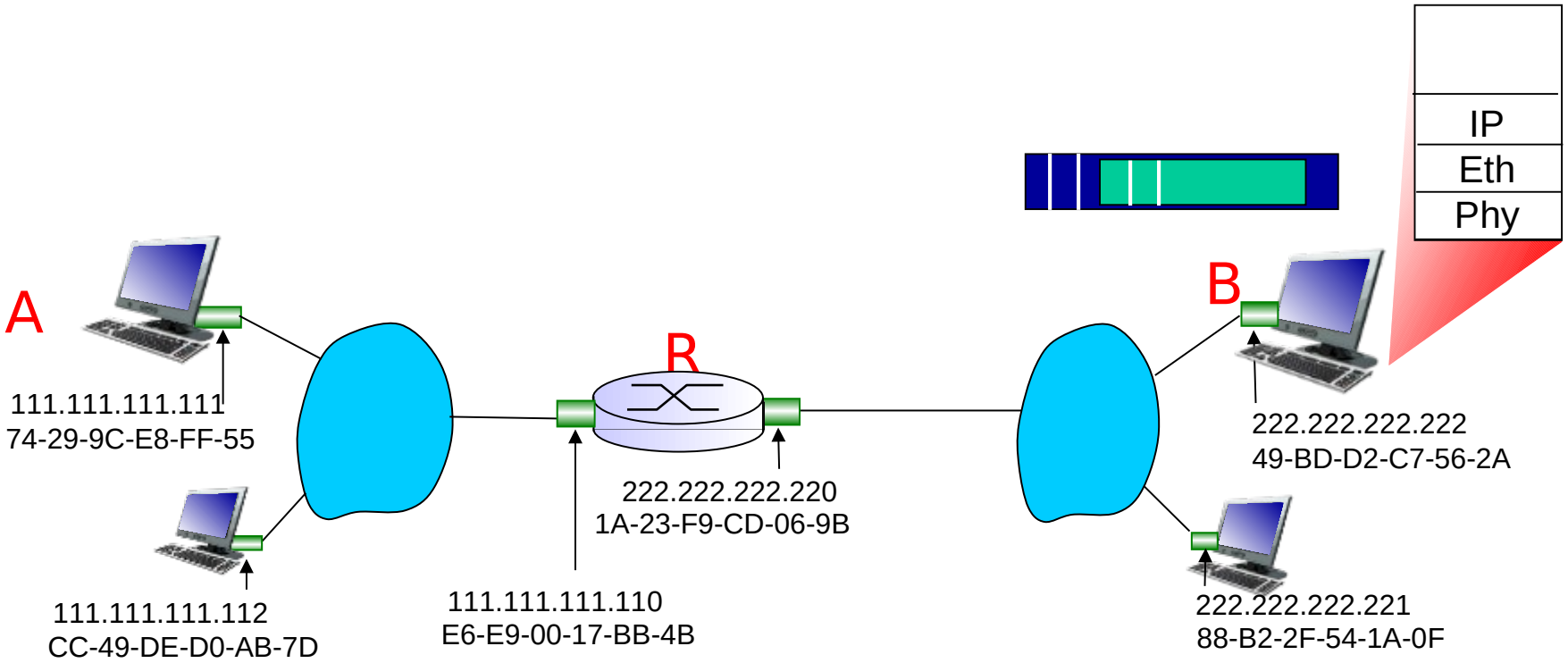
Ejemplo: enrutamiento hacia otra LAN (cont)

- R en su tabla de rutas tendrá indicado que la red correspondiente está directamente conectada
  - Debe enviarlo a B directamente. En capa de enlace, a su dirección MAC
  - Si no tiene MAC de B, utiliza ARP



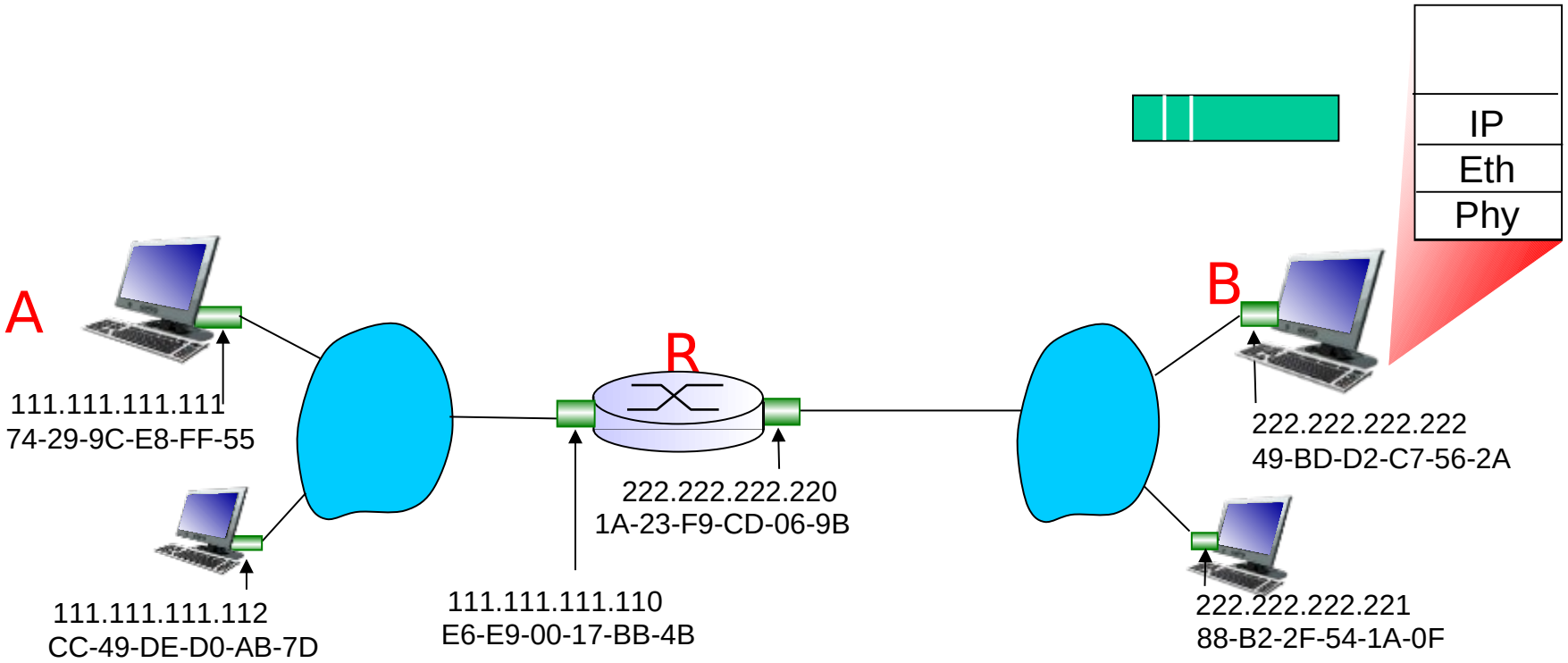
Ejemplo: enrutamiento hacia otra LAN (cont)

- B recibe en capa MAC una trama destinada a su dirección
- La envía a capa 3 (IP)
- Capa 3 procesa el paquete



Ejemplo: enrutamiento hacia otra LAN (cont)

- B recibe en capa MAC una trama destinada a su dirección
- La envía a capa 3 (IP)
- Capa 3 procesa el paquete



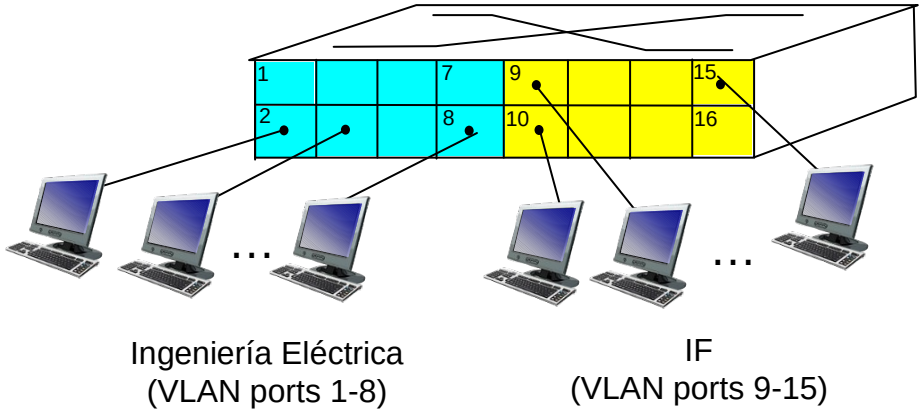
Virtual Local Area Networks (VLANs)

- La estructura “plana” de una red Ethernet con switches tiene algunas ventajas
  - Comunicación directa entre cualquier par de máquinas
  - Eficiencia, velocidad
- Y desventajas
  - Comunicación directa entre cualquier par de máquinas …
    - Falta de segregación de tráfico puede generar problemas de seguridad
    - Tráfico de broadcast y tramas a destinos aún no aprendidos bajan performance
  - Uso ineficiente de los switches si queremos separar el tráfico de distintos grupos (un switch por grupo)
    - Y dificultades de gestión (cableado) si un terminal se debe mover de grupo

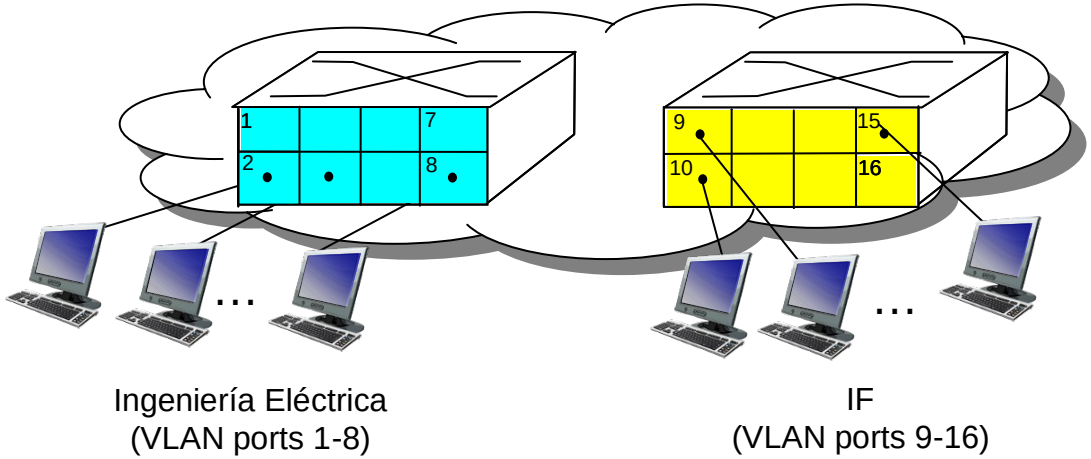
VLANs

- Idea: separar una misma infraestructura física en múltiples LANs virtuales
- Ejemplo: vlans por puerto

Estructura física

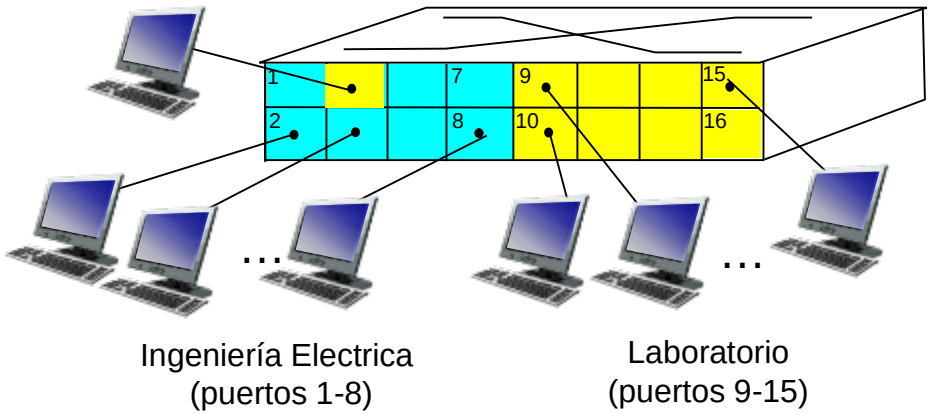


Estructura lógica



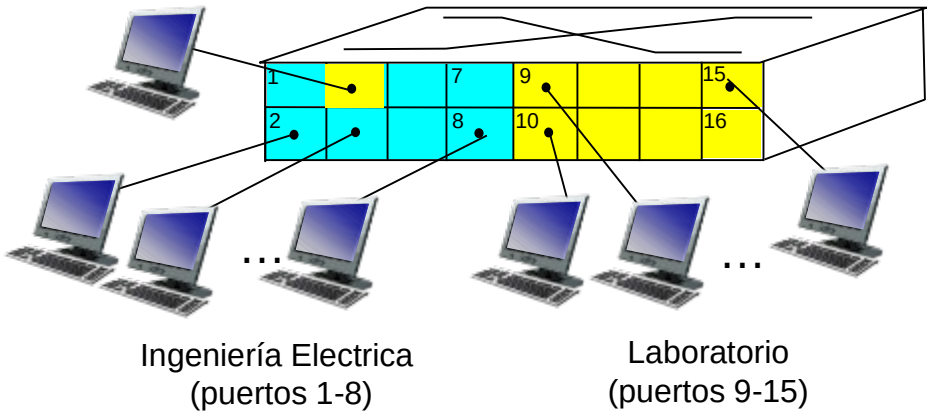
Ventajas de utilizar VLANs

- Seguridad: correctamente implementado, los equipos de una VLAN no pueden comunicarse con los de otra
  - En el ejemplo, los equipos conectados en los puertos 1-8 no pueden acceder a los equipos en los puertos 9-16
- Eficiencia: los paquetes broadcast de una VLAN no llegan a otras
- Flexibilidad: los puertos pueden asignarse a distintas vlans según conveniencia



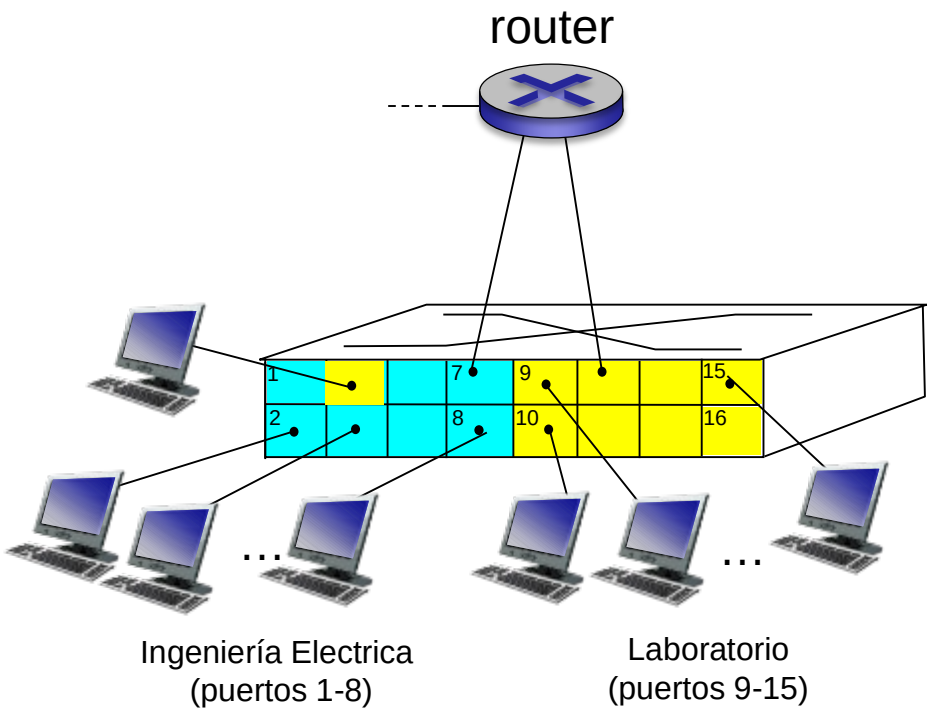
Ventajas de utilizar VLANs

- Seguridad: correctamente implementado, los equipos de una VLAN no pueden comunicarse con los de otra
  - En el ejemplo, los equipos conectados en los puertos 1-8 no pueden acceder a los equipos en los puertos 9-16
- Eficiencia: los paquetes broadcast de una VLAN no llegan a otras
- Flexibilidad: los puertos pueden asignarse a distintas vlans según conveniencia
- Interconexión entre vlans:



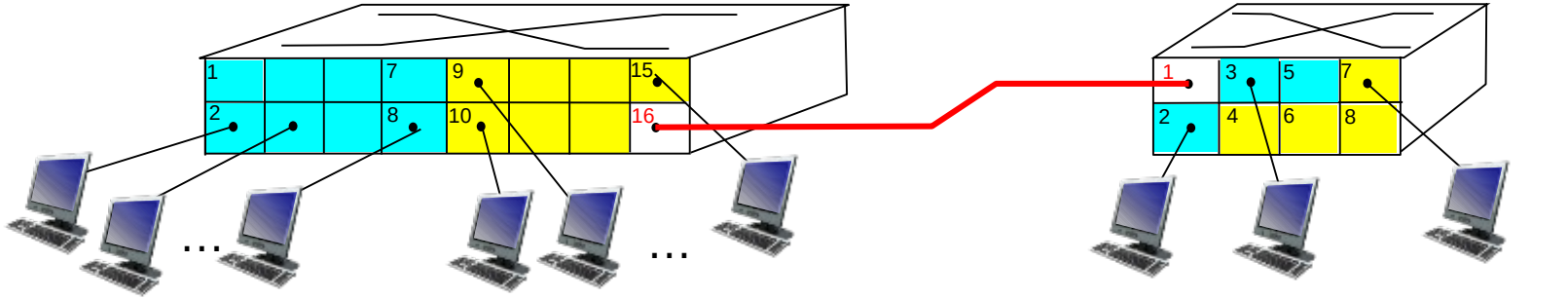
Ventajas de utilizar VLANs

- Seguridad: correctamente implementado, los equipos de una VLAN no pueden comunicarse con los de otra
  - En el ejemplo, los equipos conectados en los puertos 1-8 no pueden acceder a los equipos en los puertos 9-16
- Eficiencia: los paquetes broadcast de una VLAN no llegan a otras
- Flexibilidad: los puertos pueden asignarse a distintas vlans según conveniencia
- Interconexión entre vlans:
  - Router



Vlans entre distintos switches

- ¿Cómo distribuir la información de vlans entre switches?
  - Vlan trunking
  - Puertos que llevan la información de vlan en las tramas
  - No pueden ser tramas comunes, precisamos llevar la información del “color” de la vlan en cada trama
  - 802.1Q

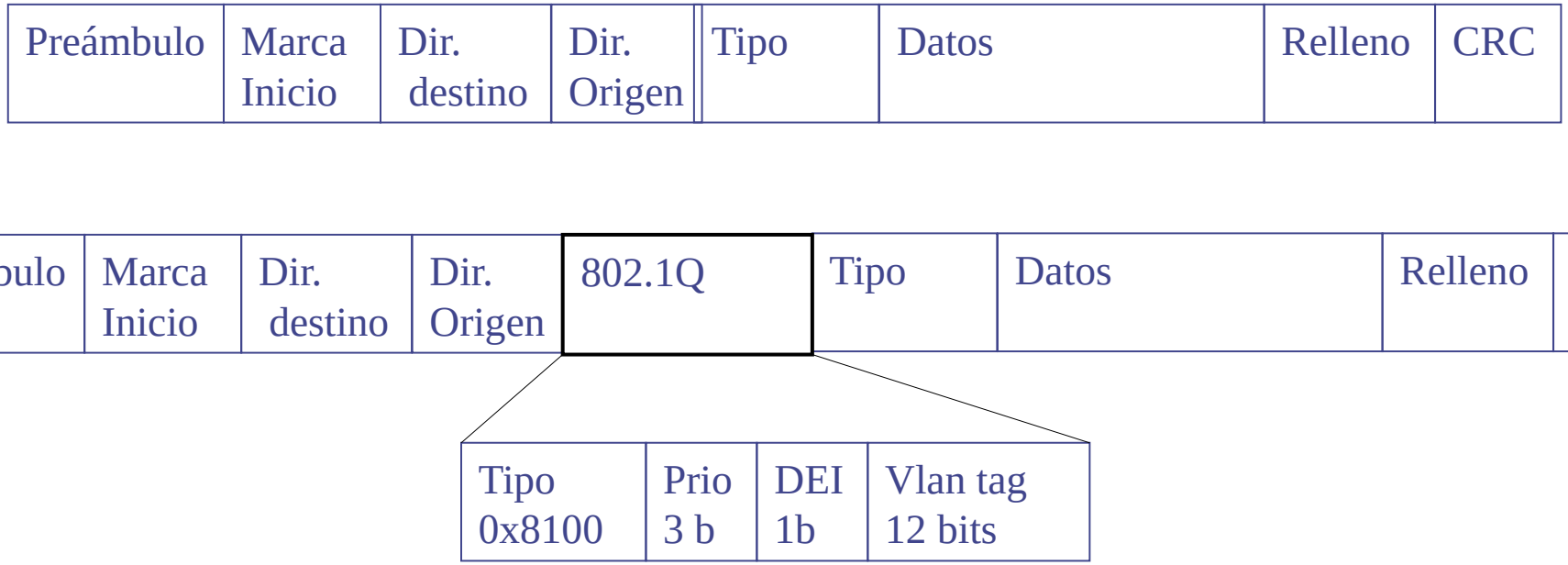


Ingeniería Electrica
(VLAN puertos 1-8)

Lab
(VLAN puertos 9-15)

Puertos 2,3,5 pertenecen a IE
Puertos 4,6,7,8 pertenecen al lab

802.1Q



- Se insertan 4 bytes entre el encabezado
- El nuevo “tipo” indica “trama con vlan”
- 12 bits para el tag de vlan → hasta 4096 vlans
- Prio: utilizado para llevar información de prioridad (hasta 8 niveles)

802.1Q (cont)

- No es necesario que las máquinas entiendan de vlans. Solo los switches
  - En muchos casos se usa en enrutadores y hosts
- Trama más grande que 1500 bytes. Debe ser soportado

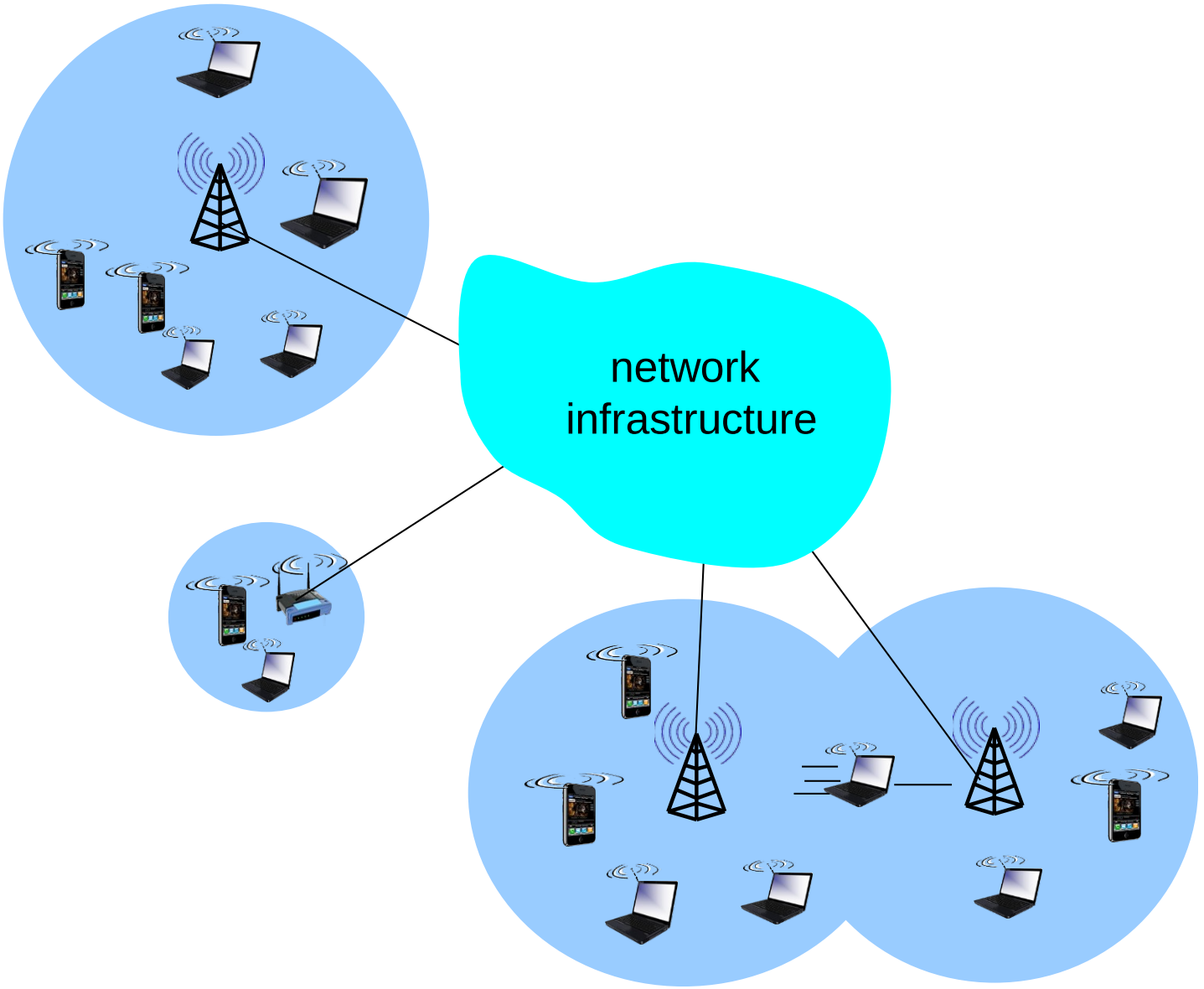
Redes inalámbricas

Facultad de Ingeniería – Universidad de la República

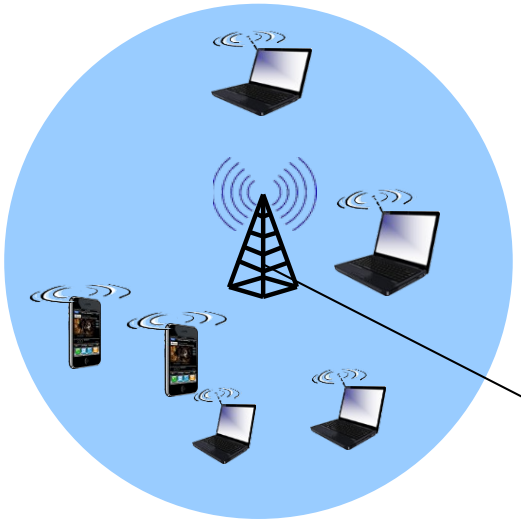
Redes inalámbricas

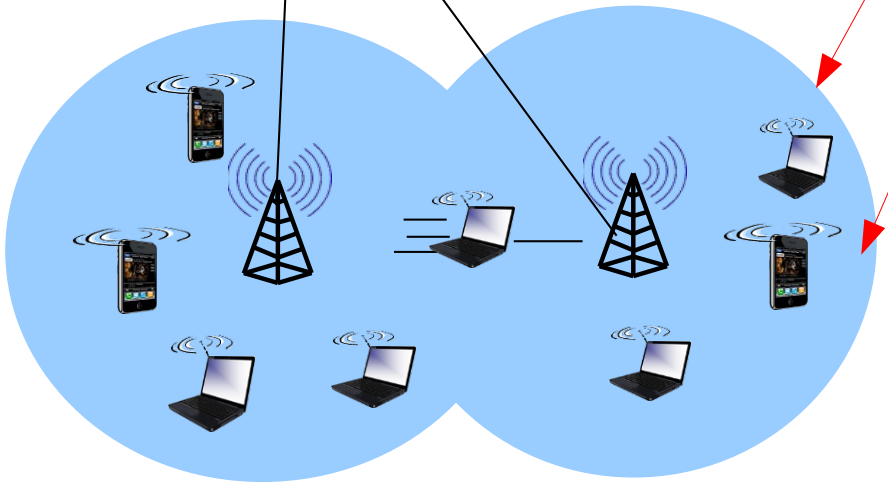
- Redes donde se envían señales en el espectro electromagnético sin un soporte físico (sin cables ni fibras)
- Múltiples tecnologías con muy variadas capacidades
- Ejemplos:
  - Redes celulares
  - Redes de área local (WiFi)
  - Redes de área personal (Bluetooth)
  - Redes específicas para sensores (LoraWAN, etc)
  - etc, etc.
- Dos problemas relacionados:
  - Comunicación por un link inalámbrico
  - Movilidad

Elementos de una red inalámbrica



Elementos de una red inalámbrica



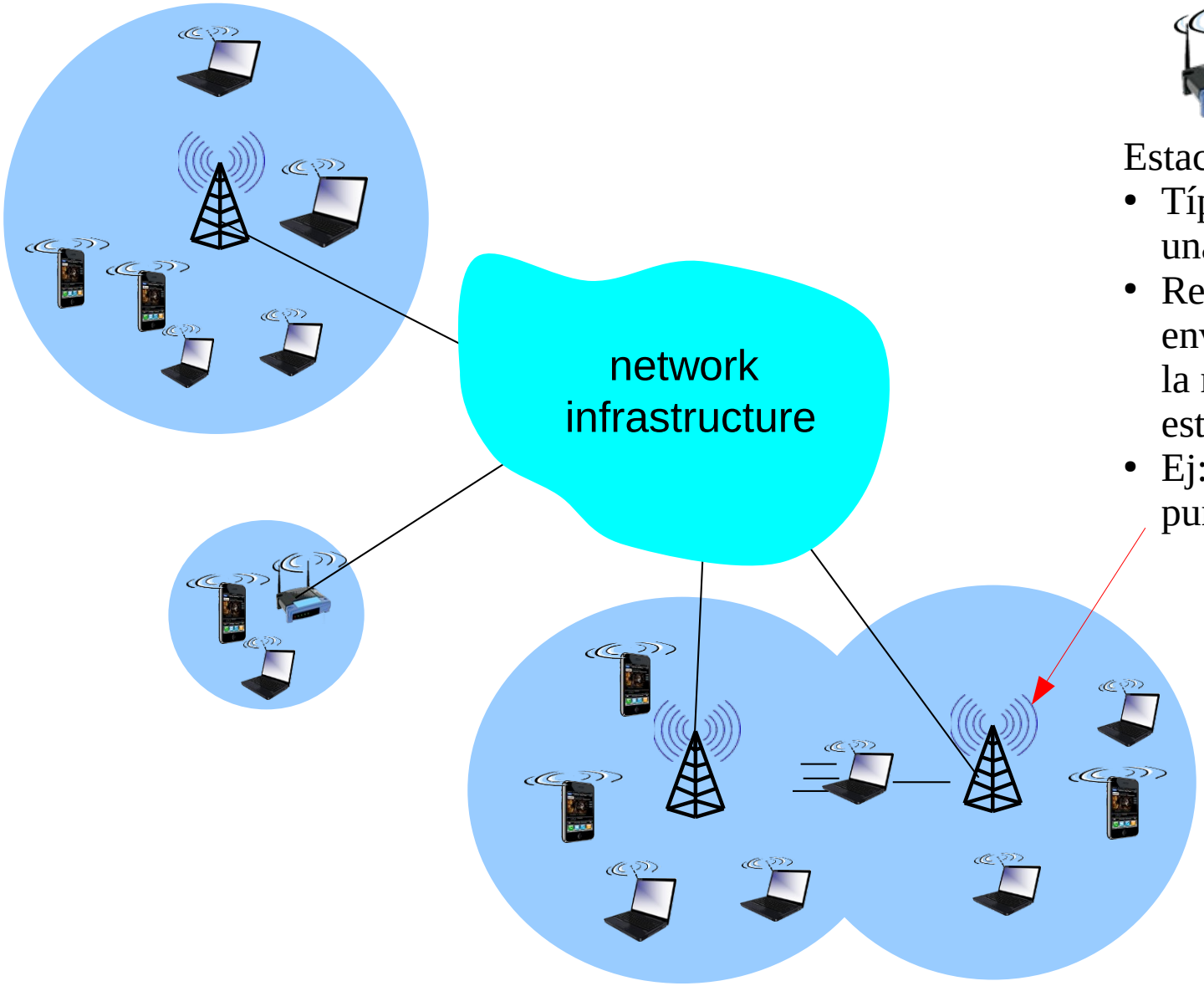


network infrastructure

Hosts inalámbricos

- Laptops, teléfonos
- Corren aplicaciones
- Pueden ser estacionarios o móviles

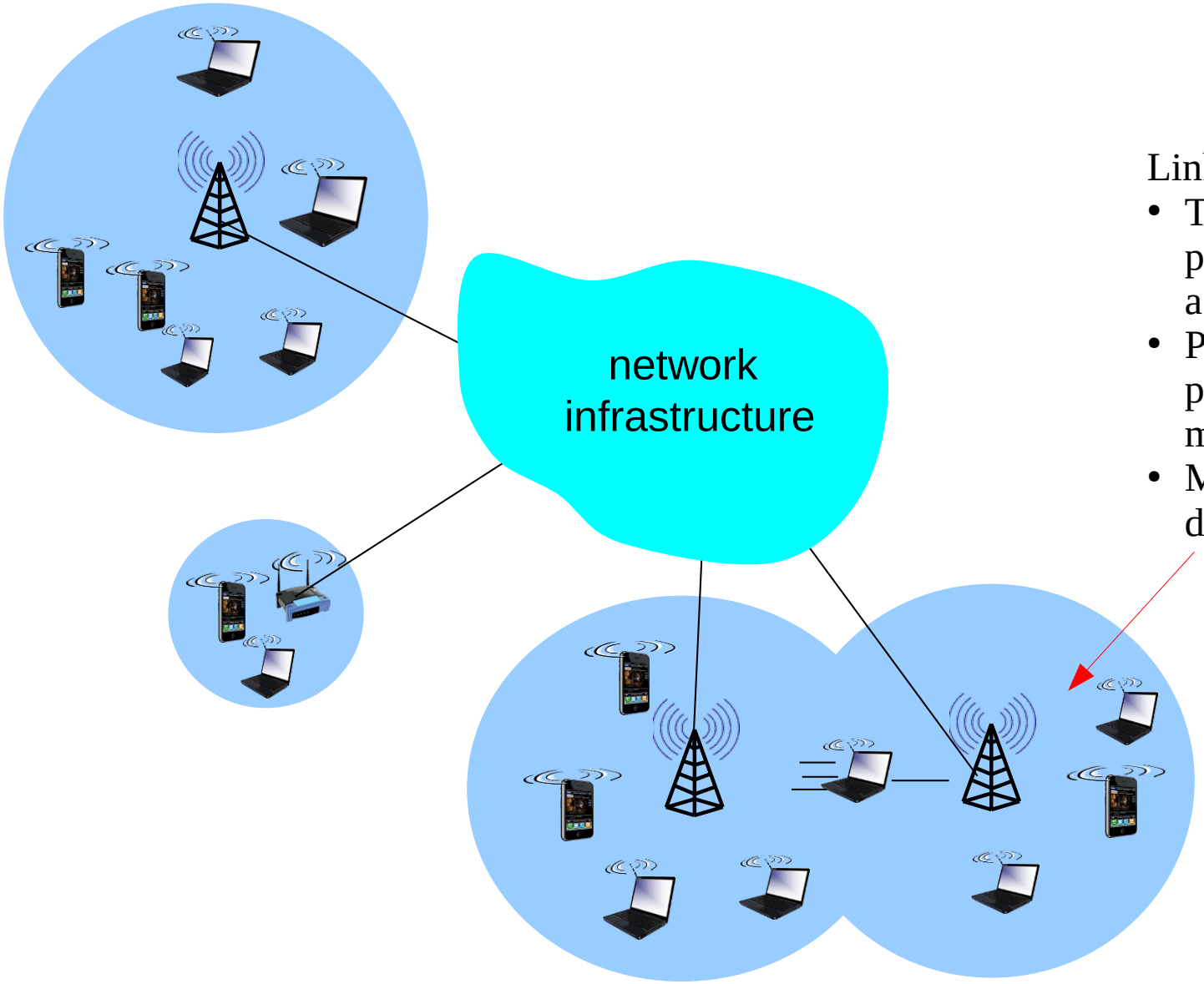
Elementos de una red inalámbrica



Estaciones Base

- Típicamente conectada a una red cableada
- Relay. Responsable de enviar los paquetes entre la red fija y las estaciones móviles
- Ej: Torres celulares, puntos de acceso 802.11

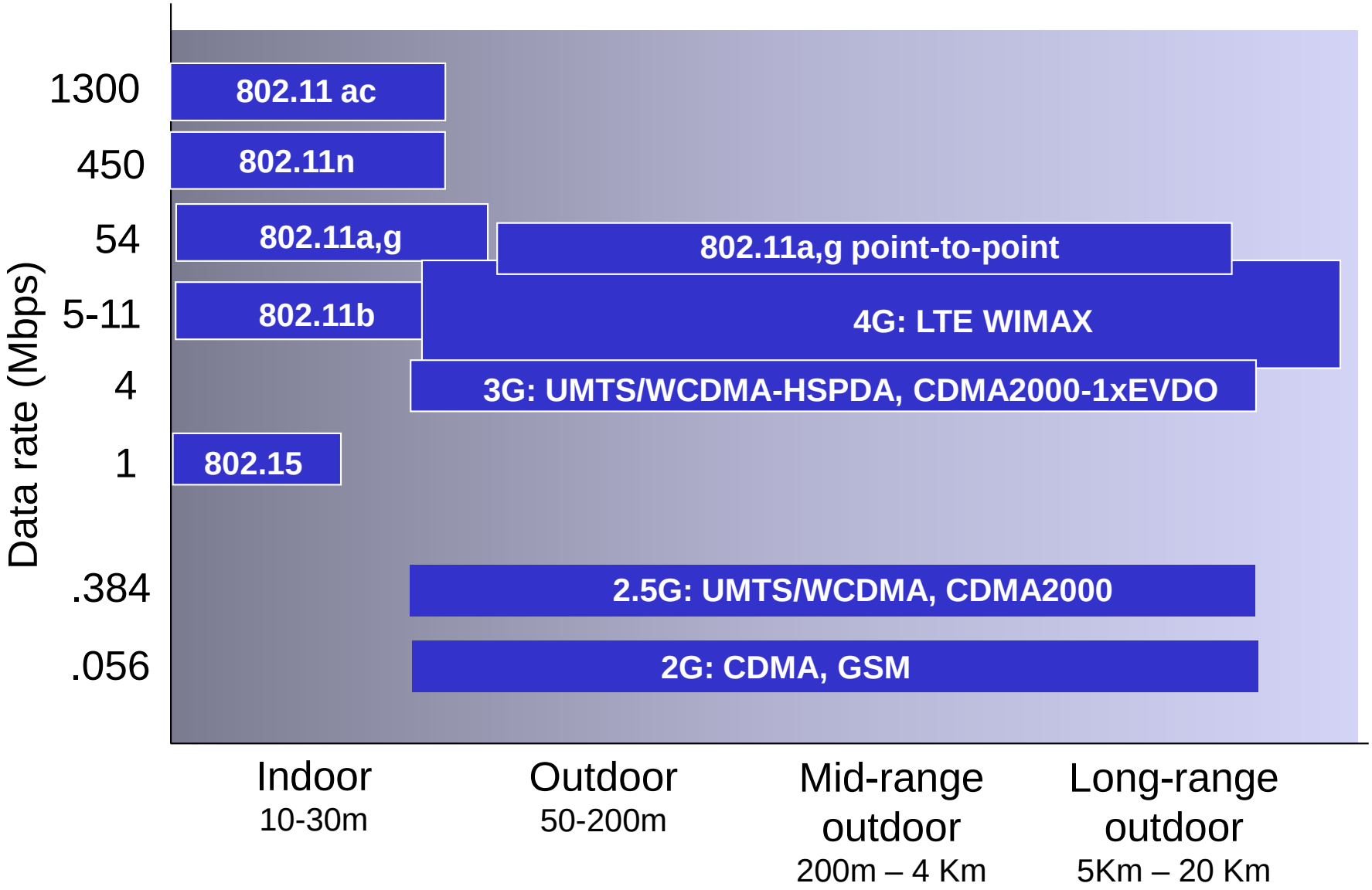
Elementos de una red inalámbrica



Links inalámbricos

- Típicamente utilizados para conectar estaciones a las bases
- Protocolos de acceso para coordinar acceso al medio
- Múltiples data rates, distancias...

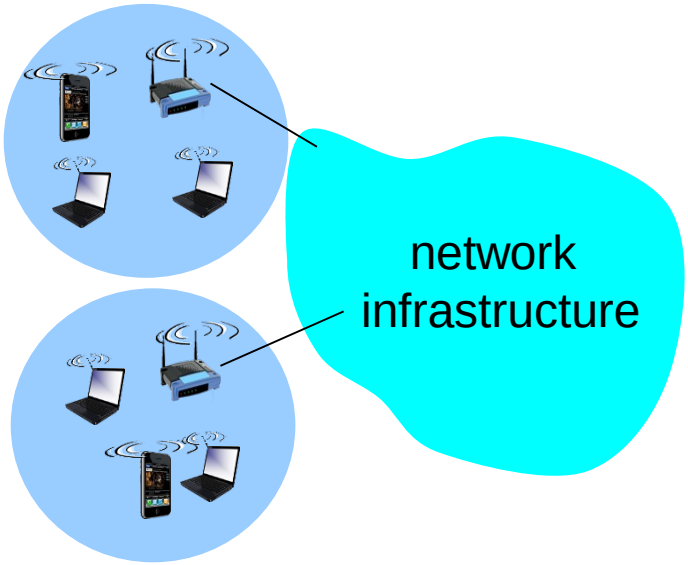
Ejemplos de algunas redes



Modo infraestructura vs. modo ad-hoc

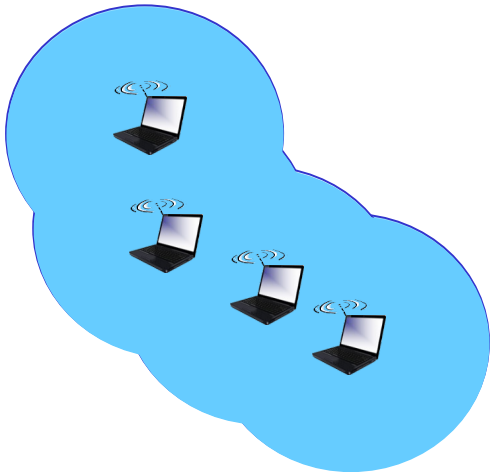
Modo infraestructura

- Estaciones base (p. ej. Access points) dan servicio a un grupo de estaciones
- Brinda conectividad, asignación de direcciones, etc.



Modo ad-hoc

- No hay infraestructura
- La red se arma entre los hosts que están dentro del alcance

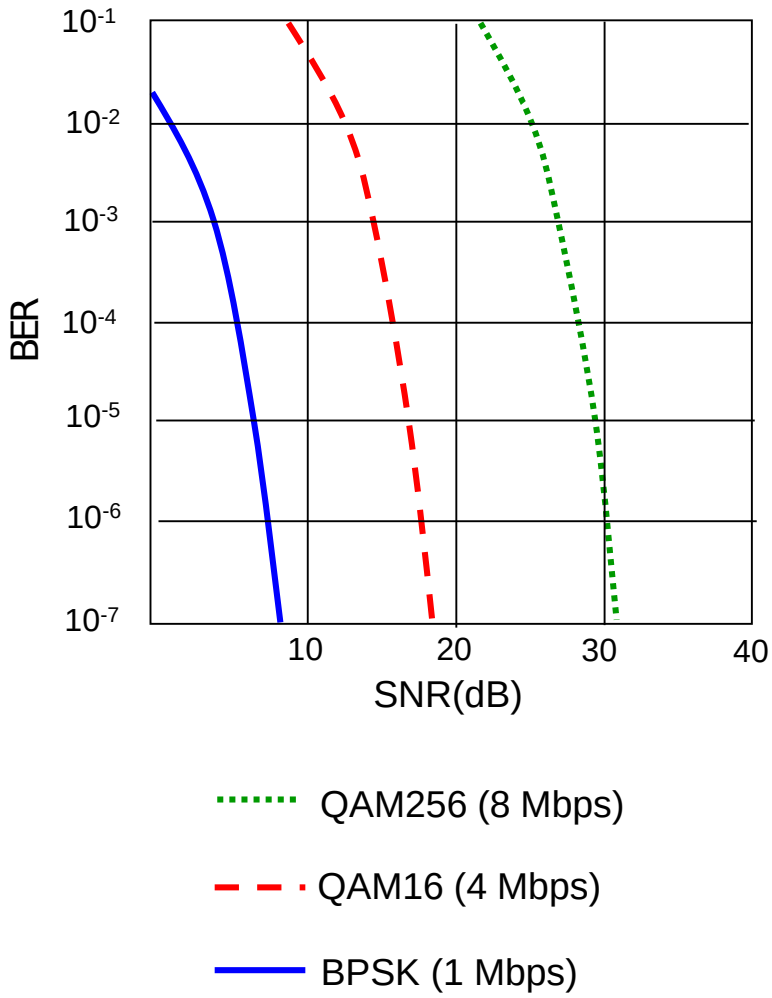


Características de los medios inalámbricos

- Diferencias importantes con las redes cableadas:
  - Atenuación. La señal se atenúa al propagarse, y al atravesar obstáculos
  - Interferencia de otras fuentes. Fuentes transmitiendo en la misma banda de frecuencias se interferirán
    - WiFi trabaja en frecuencias “libres”: muchos equipos trabajando en las mismas frecuencias
    - Ruido electromagnético de otras fuentes (motores, microondas, etc)
  - Propagación multicamino. Sucede cuando parte de la onda electromagnética se refleja en objetos o el piso, tomando caminos de distinta longitud. Esto provoca interferencia en el receptor
  - Otros
- Mayores tasas de error
- Calidad variable

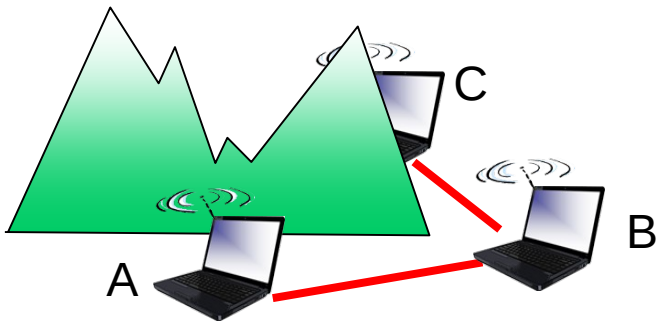
Características: SNR

- Signal to Noise Ratio:
  - Medida de la potencia de señal vs potencia del “ruido”
  - Mayor SNR: “mejor” (más fácil recuperar señal sin error)
  - Distintas modulaciones: compromiso throughput – errores
  - Situaciones de movilidad: modulación adaptativa



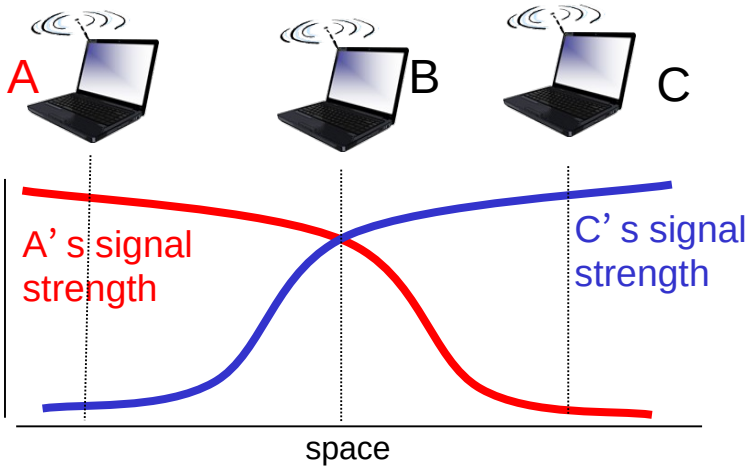
Interferencia en el receptor

- Además de los problemas vistos por el acceso al medio compartido, problemas debidos a la propagación de la señal: estaciones ocultas



Estaciones ocultas por obstáculos:

- B y A se escuchan
- B y C se escuchan
- A y C no se escuchan, no se dan cuenta que se interfieren en B



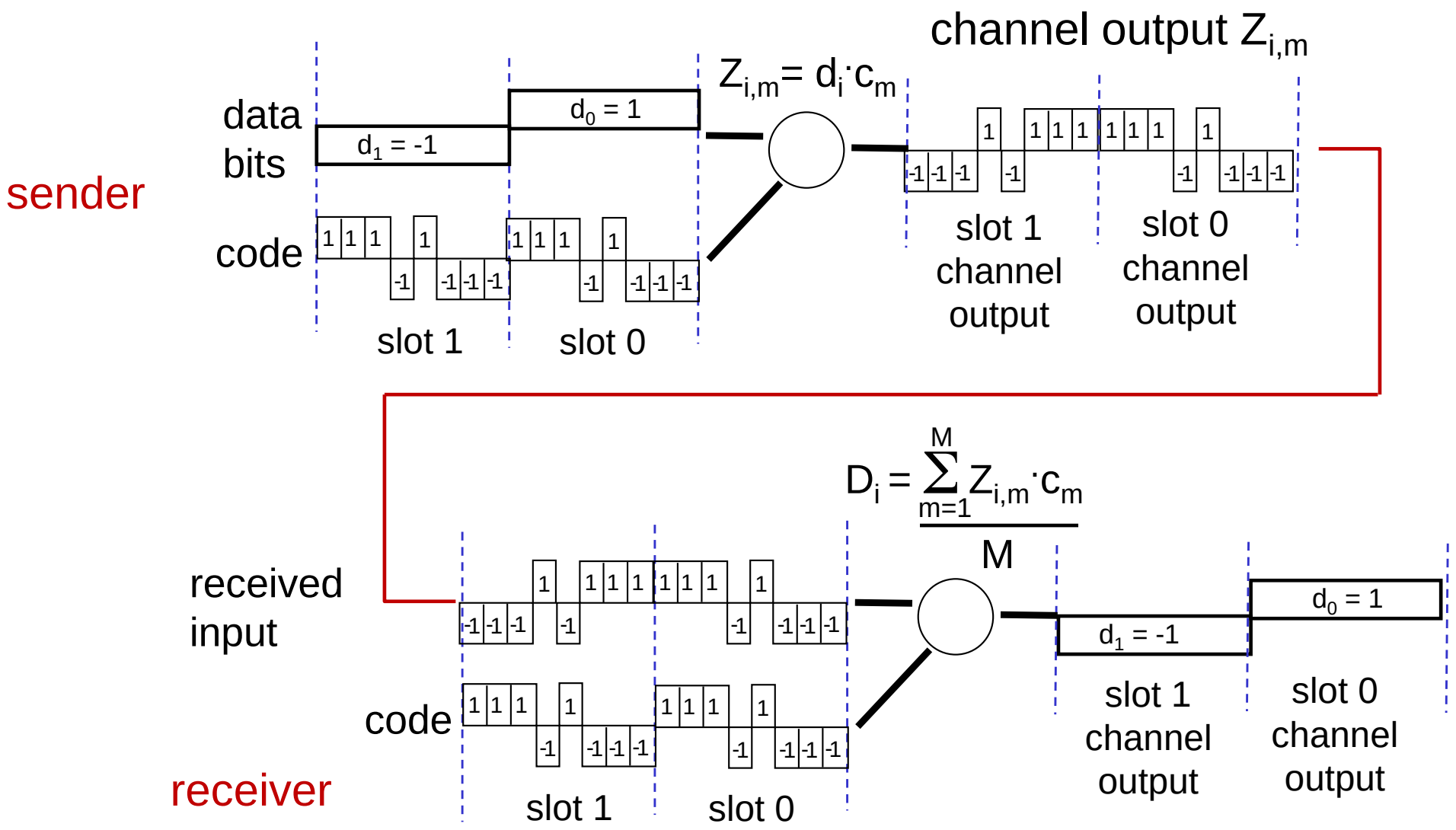
Estaciones ocultas por atenuación

- B y a se escuchan
- B y C se escuchan
- A y C no se escuchan, no se dan cuenta que se interfieren en B

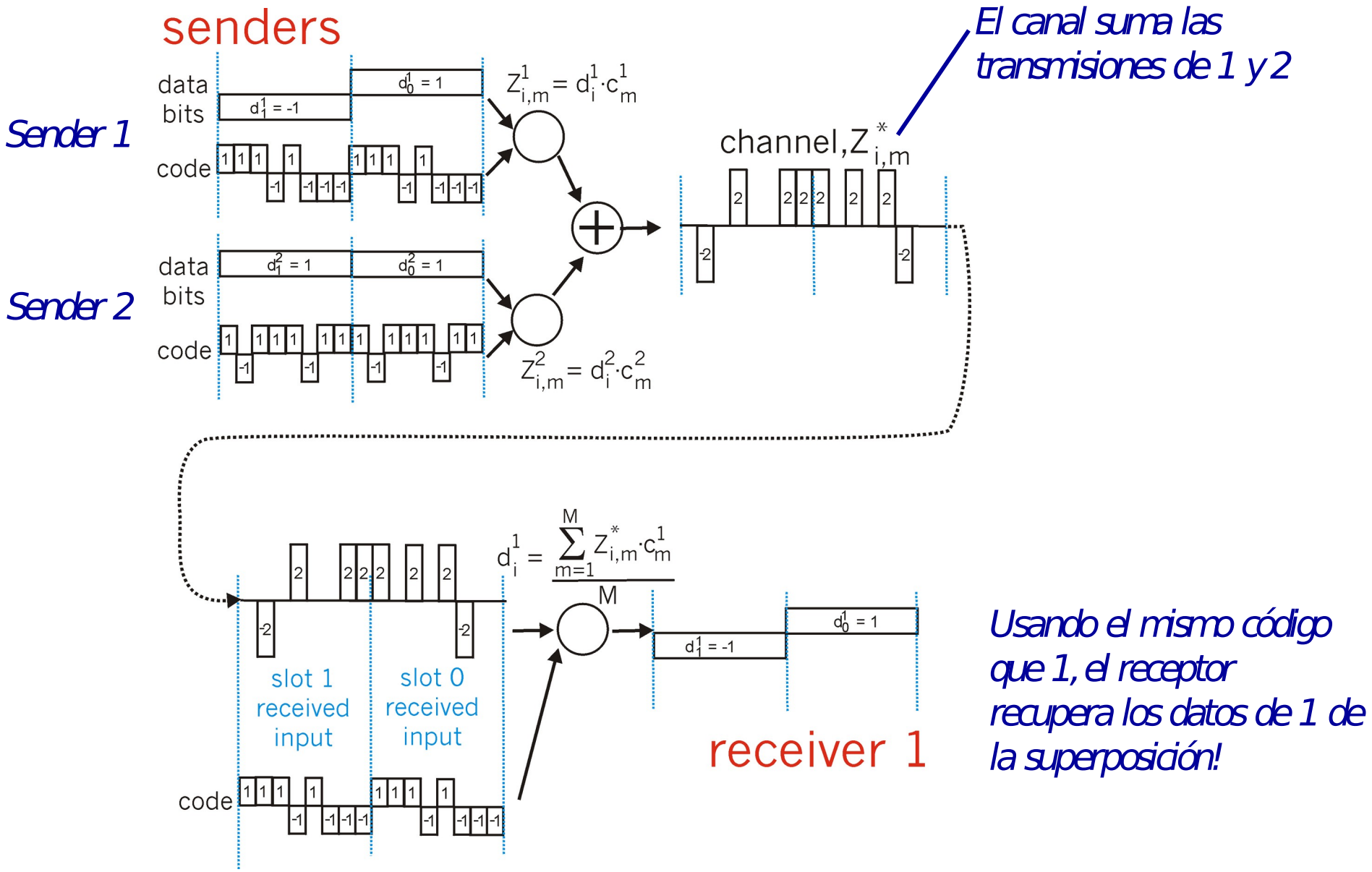
CDMA (Code Division Multiple Access)

- Modo de particionar el medio, donde a cada estación se le asignan uno o más códigos
  - Todas las estaciones comparten el medio, pero a cada una se le asigna un código distinto (chipping sequence)
  - Permite a múltiples usuarios coexistir en el medio y transmitir simultáneamente con interferencia mínima (códigos ortogonales)
  - División del canal por código. Si el código se asigna estáticamente, similar a otras divisiones estáticas del canal
- Codificación: (datos originales) x (chipping sequence)
- Decodificación: producto interno de la secuencia codificada con chipping sequence

CDMA: Codificación/decodificación



CDMA con múltiples transmisores



CDMA

- Sistemas que utilizan variantes de CDMA:
  - Redes celulares 3G (asignación dinámica de códigos de largo variable)
  - 802.11 (WiFi) en algunas de sus modulaciones
  - Algunas redes para el “Internet de las cosas” (LoRaWan y otras)

Redes 802.11 (WiFi)

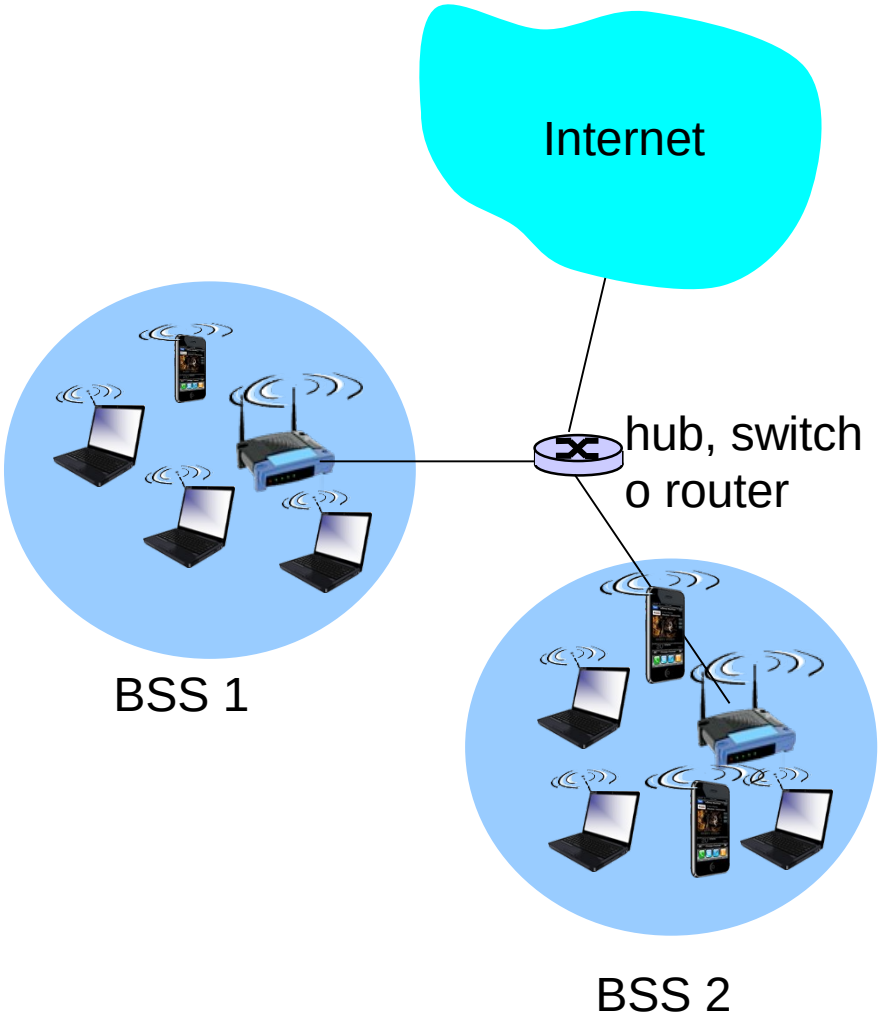
- Redes de área local inalámbricas
- Utilizan rangos de frecuencia reservados para uso sin licencia
  - 2.4 GHz (2400-2483 MHz)
  - 5,8 GHz (5725-5850 MHz)
- Deben ser resistentes a interferencia, ruido, etc
- Deben solucionar el acceso al medio compartido
- Deben solucionar el problema de las estaciones ocultas

Diferentes versiones

- 802.11. 2,4 GHz, 1-2 Mbps (max)
- 802.11b – 2,4 GHz, 11 Mbps
- 802.11a – 5,8 GHz, 54 Mbps
- 802.11g – 2,4 GHz, 54 Mbps
- 802.11n – 2,4, 5,8 GHz – 200 Mbps. ¿600 Mbps?
- 802.11ac - > 1 Gbps
- Todas velocidades máximas, en condiciones óptimas

Arquitectura

- Estación base: Access Point (AP)
- Los hosts se comunican con el Access Point, y no directamente entre ellos
- BSS (Basic Service Set): conjunto de un AP y las estaciones conectadas a el
- Existe también un modo “ad-hoc”, donde las estaciones se conectan directamente sin AP



802.11: canales y frecuencias, asociación

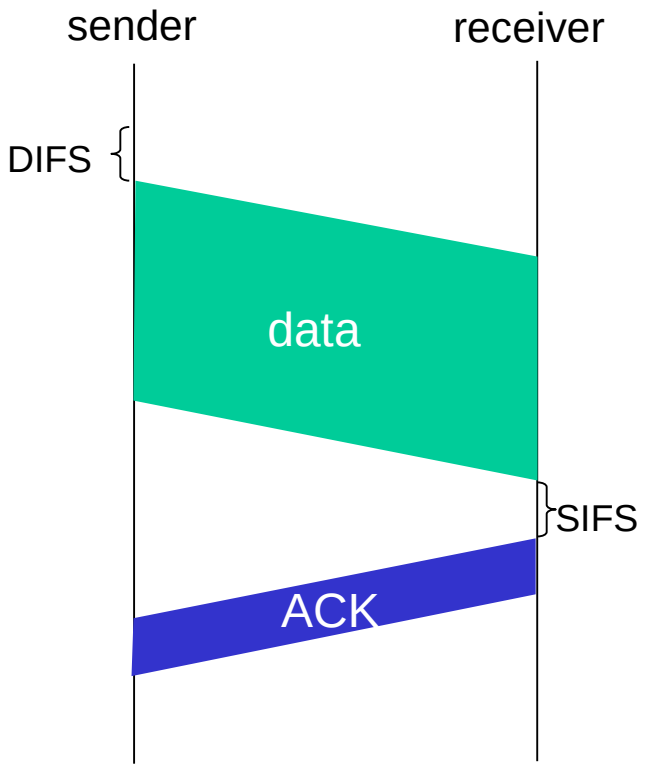
- Ej 802.11b: el espectro disponible (2,4 – 2,485 GHz) se divide en canales (11-12 dependiendo de la región)
- El canal a utilizar se configura administrativamente en el AP
  - Algunos APs pueden elegirlo automáticamente
- Interferencia posible con APs cercanos
- No todos los canales son disjuntos
- Los hosts deben asociarse con el AP
  - Scan: escucha sucesivamente todos los canales, buscando tramas específicas (beacon frames) que contienen el nombre (SSID) de la red y la MAC del AP
    - Es posible enviar un “Probe” (pedido de AP)
  - Selecciona un AP
  - Realiza autenticación (a menos que sea una red abierta)
  - Una vez asociado (y autenticado), obtendrá IP, GW, DNS usando DHCP

Acceso múltiple: CSMA/CA

- CSMA: sensar el canal antes de transmitir
- No hay detección de colisiones (CD)
  - Muy difícil escuchar mientras se transmite (señales muy débiles)
  - Hay casos que no podemos resolver (estación oculta)
  - Intentaremos evitar las colisiones
    - CSMA/CA (Collision Avoidance)
- No tenemos detección de colisiones: agregamos ACK
  - Además tenemos altas tasas de error
- Varios timers (SIFS, DIFS, etc)

802.11 CSMA/CA (1)

- Transmisor:
  - Si se observa el canal libre durante DIFS, entonces transmite la trama
    - Si no se recibe ACK, debe retransmitirse
  - Si se observa el canal ocupado:
    - Random backoff time
    - Si el canal está libre, transmitir cuando vence el timer
    - Si no hay ACK, incrementar el tiempo de backoff y actuar como canal ocupado
- Receptor:
  - Si se recibe trama correctamente:
    - Esperar SIFS y devolver ACK

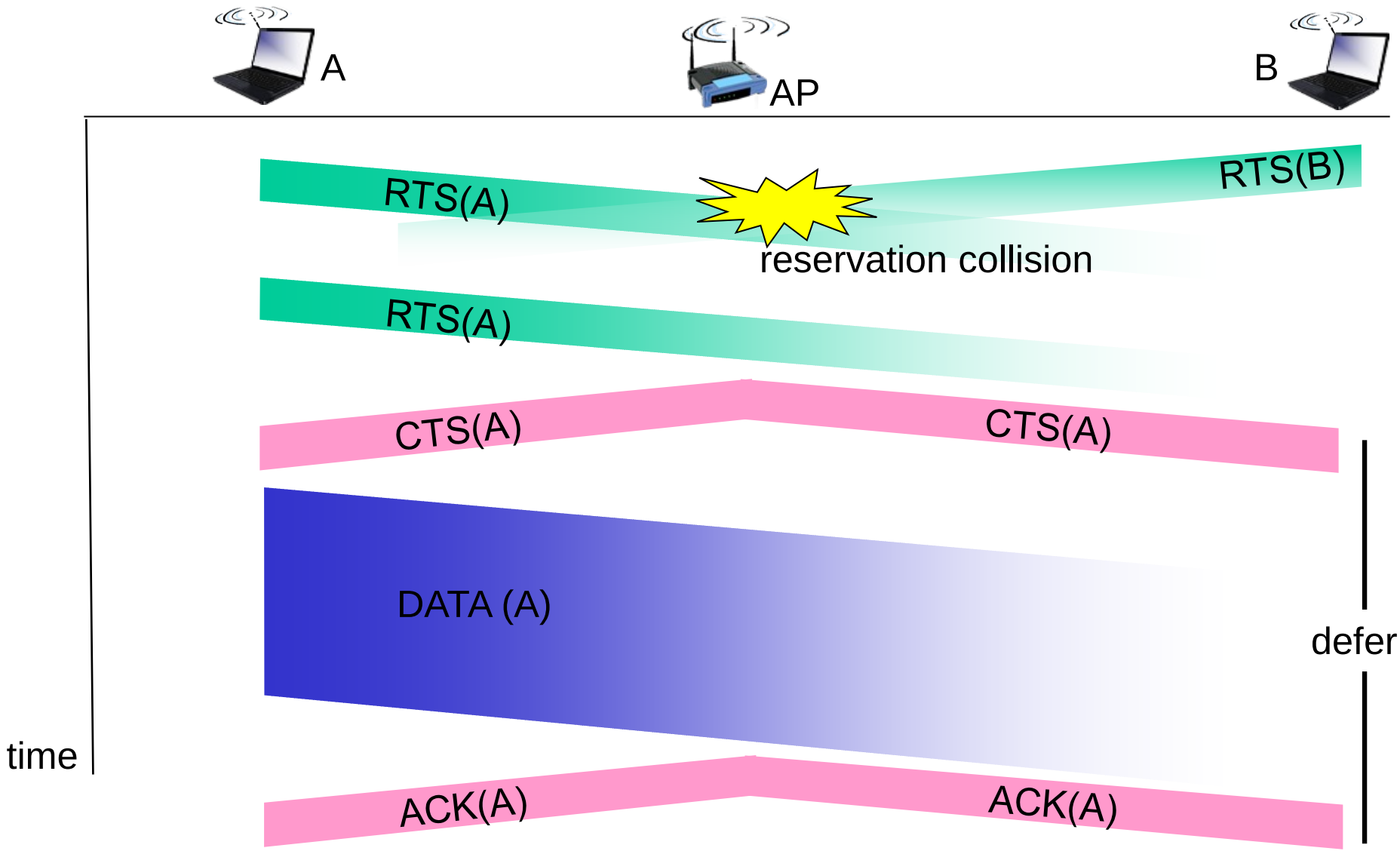


802.11 CSMA/CA (2)

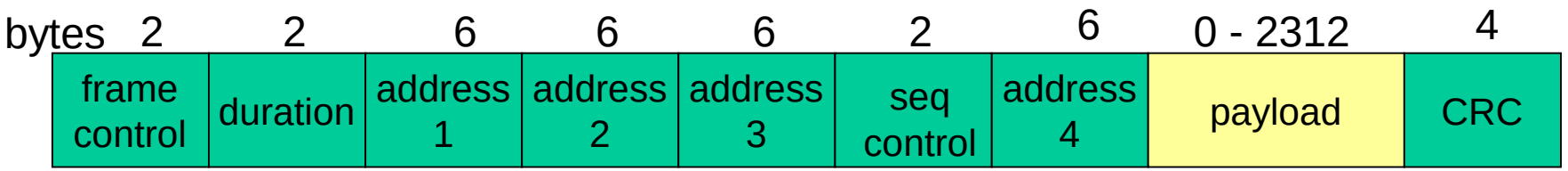
- Para evitar colisiones (CA), queremos poder reservar el canal para evitar colisión de tramas largas
- Transmisor A envia trama de reserva (RTS) corta destinada a receptor (B)
  - Pueden colisionar
- Receptor envía confirmación (CTS) también corta
- CTS escuchada por todos los nodos cercanos al receptor:
  - Estaciones cercanas al receptor se abstendrán de transmitir
  - A podrá transmitir sin colisiones

- Observación: CSMA/CA es opcional
- Observación: solo se usa para tramas largas

CSMA/CA

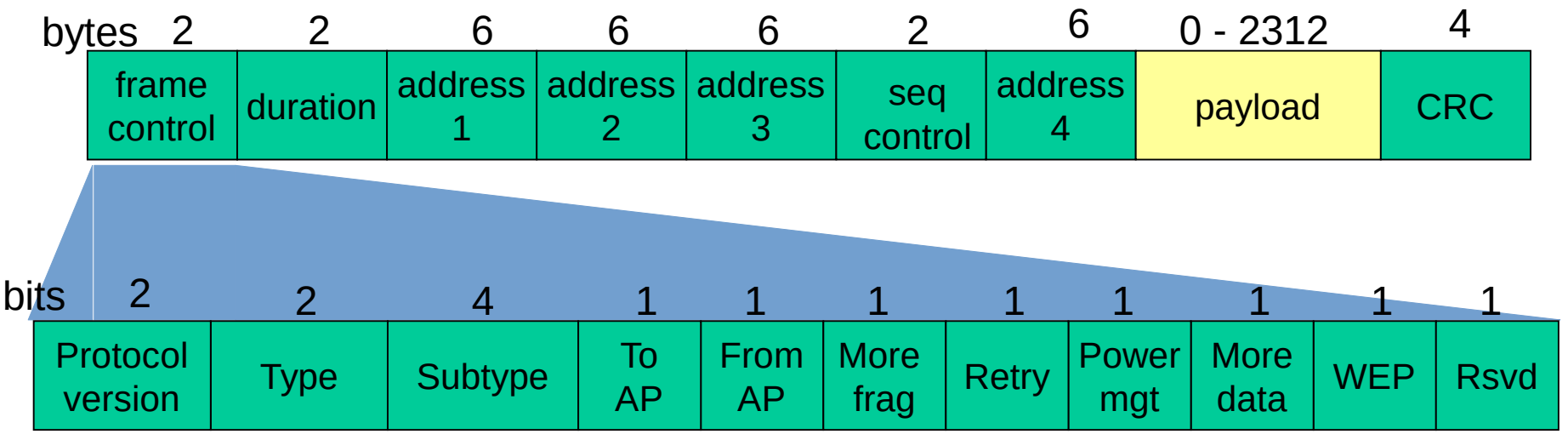

A
AP
B
RTS(A)
RTS(B)
reservation collision
RTS(A)
CTS(A)
CTS(A)
DATA (A)
defer
time
ACK(A)
ACK(A)

Trama 802.11



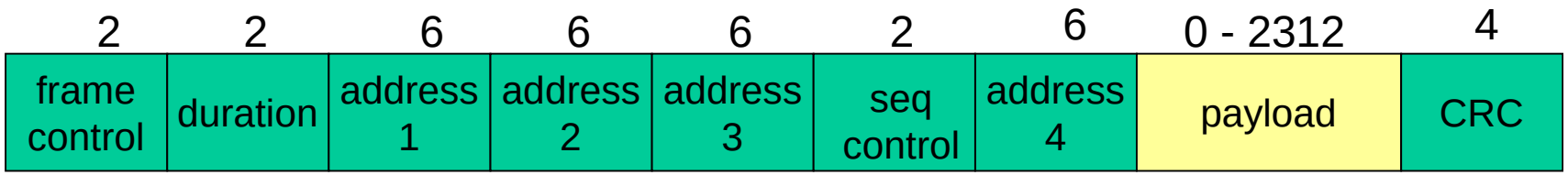
- Payload: carga útil de la trama
- CRC: detección de errores, 32 bits
- Duration: indicación de la duración de la reserva del canal (tanto en tramas de datos, como en RTS/CTS)
- Seq: número de secuencia (para tramas de datos). 12 bits (secuencia) + 4 bits (número de fragmento si fragmentamos)
  - Permite controlar duplicados en caso de retransmisión

Trama 802.11: Frame Control



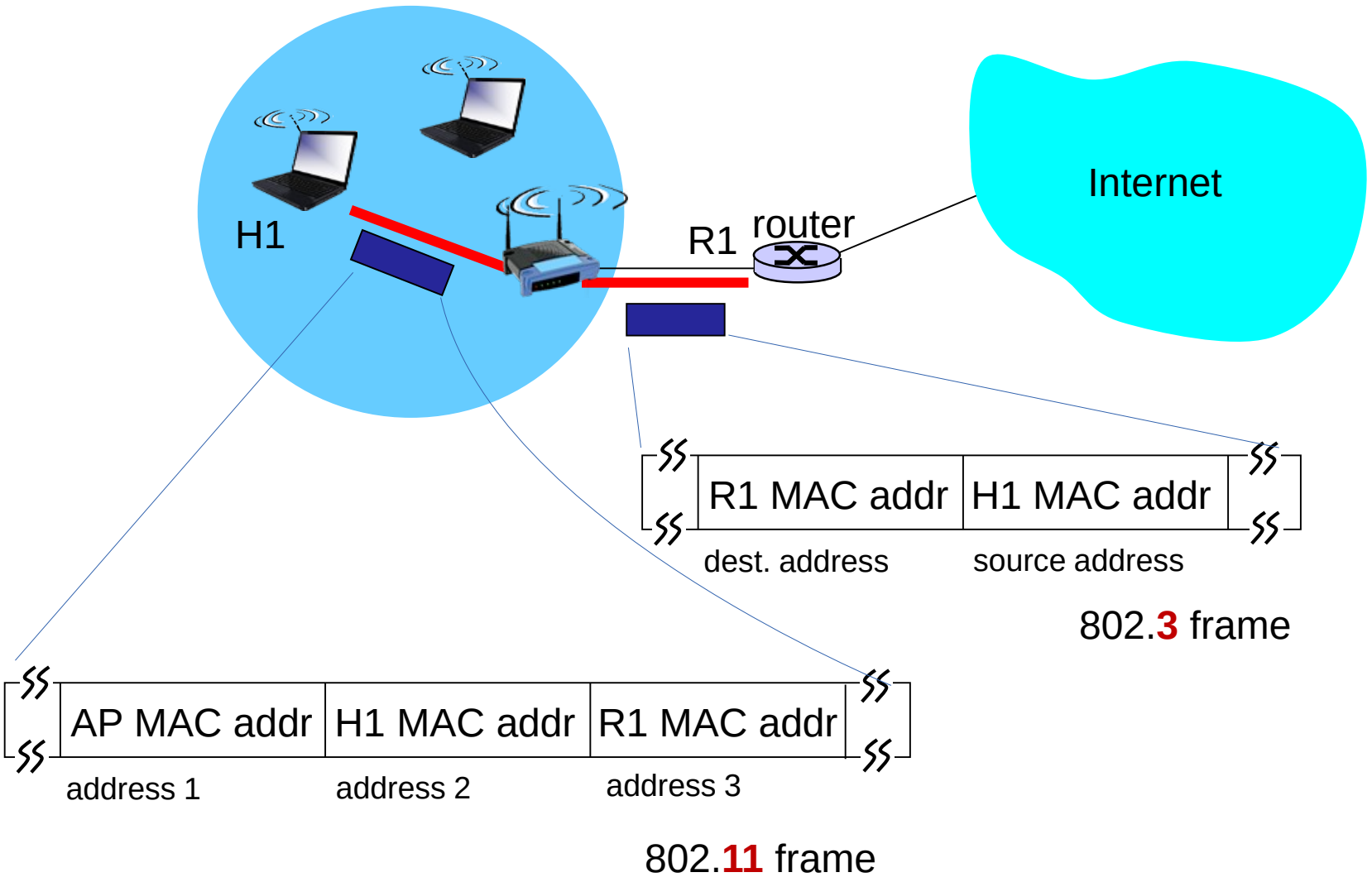
- Versión: 00
- Tipo y subtipo: datos, ACK, RTS, CTS, control, etc.
- To AP: trama destinada al AP
- From AP: trama con origen un AP
- More frag: hay más fragmentos de esta trama
- Retry: es una retransmisión
- ….

Trama 802.11: Direcciones



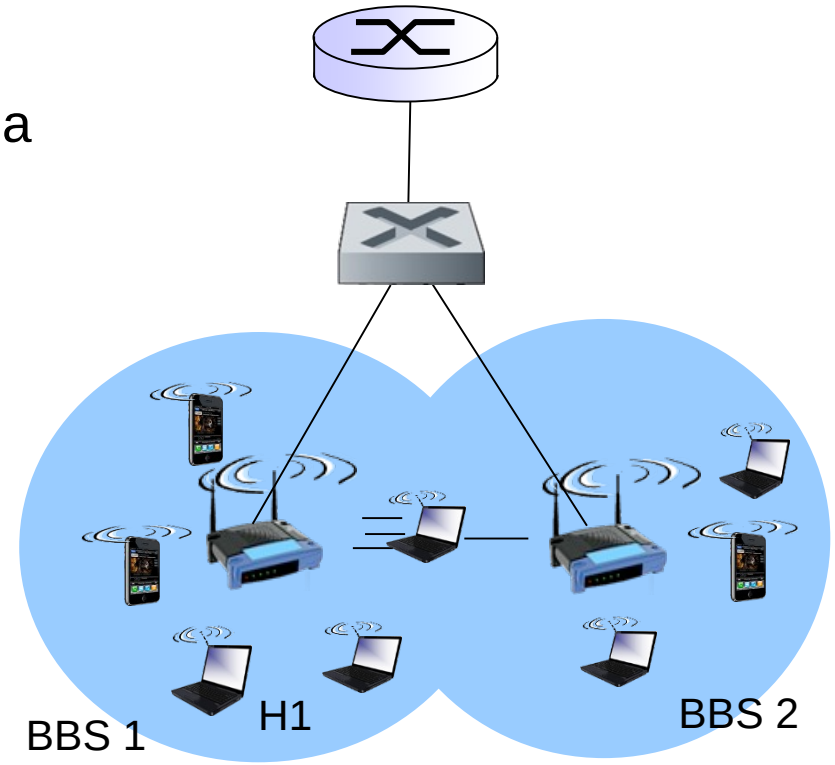
- Hasta 4 direcciones
- Address 1: destino (en el aire)
- Address 2: origen (en el aire)
- Address 3: dirección origen o destino finales
- Address 4: usada en links inalámbricos entre AP

Ejemplo


H1
R1
router
Internet
R1 MAC addr
H1 MAC addr
dest. address
source address
802.3 frame
AP MAC addr
H1 MAC addr
R1 MAC addr
address 1
address 2
address 3
802.11 frame

802.11. Movilidad dentro de la misma subred

- ¿Qué pasa si una estación se mueve de un access-point a otro?
- Si están conectados por un switch (misma subred), este aprenderá por qué link es alcanzable la estación
- Puedo mantener la IP, y todas las conexiones que tuviera establecidas



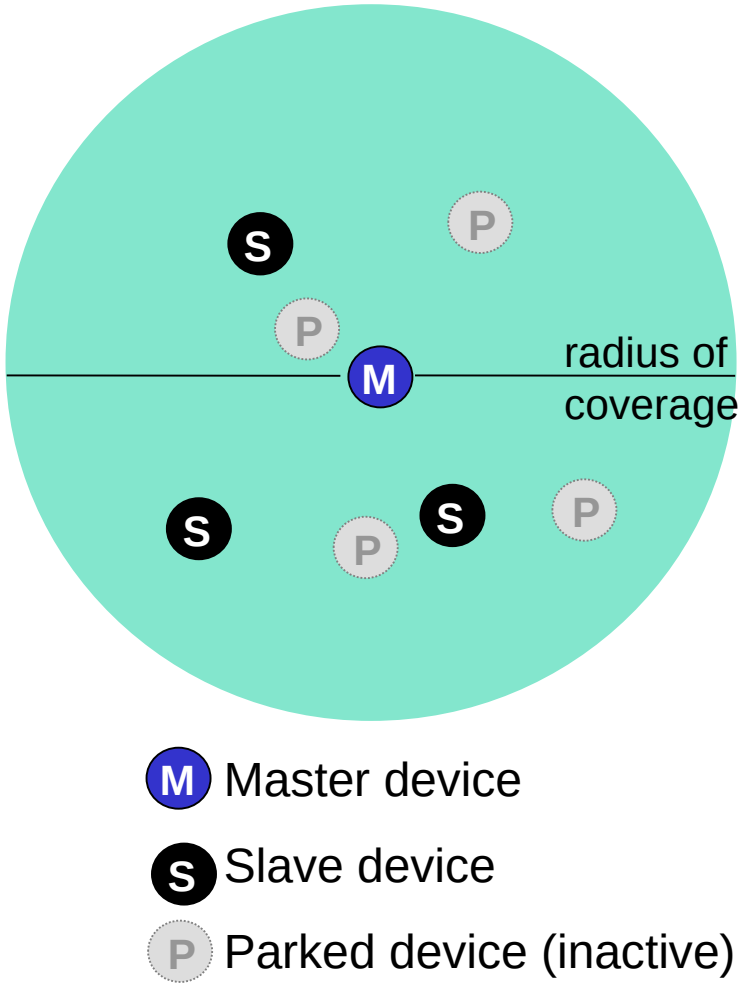
Modulación adaptativa, manejo de potencia

- ¿Qué pasa si el usuario se mueve?
- Al alejarse empeora SNR, empeora BER
- Implementaciones de modulación adaptativa
  - Ej: ante 2 pérdidas seguidas bajar modulación, ante 10 tramas reconocidas aumentar modulación

- Nodos móviles quieren ahorrar energía
- Si no tienen nada para enviar, pueden indicar que pasan a modo “sleep”
  - Apagan transmisor y receptor hasta el próximo beacon (100 ms)
- AP guarda las tramas
- En el beacon indica qué estaciones tienen tráfico para recibir
  - Si no tengo nada, vuelvo a dormir...

802.15 – personal area network

- 802.15.1: Bluetooth
- Frecuencia: banda de 2.4 GHz
- Radio < 10 mts
- “reemplazo de un cable”. Auriculares, teclado, mouse, etc
- Sin infraestructura (ad-hoc)
- master/slave. El master gobierna la red, esclavos solo pueden transmitir si el master lo indica
- Hasta 721 kbps



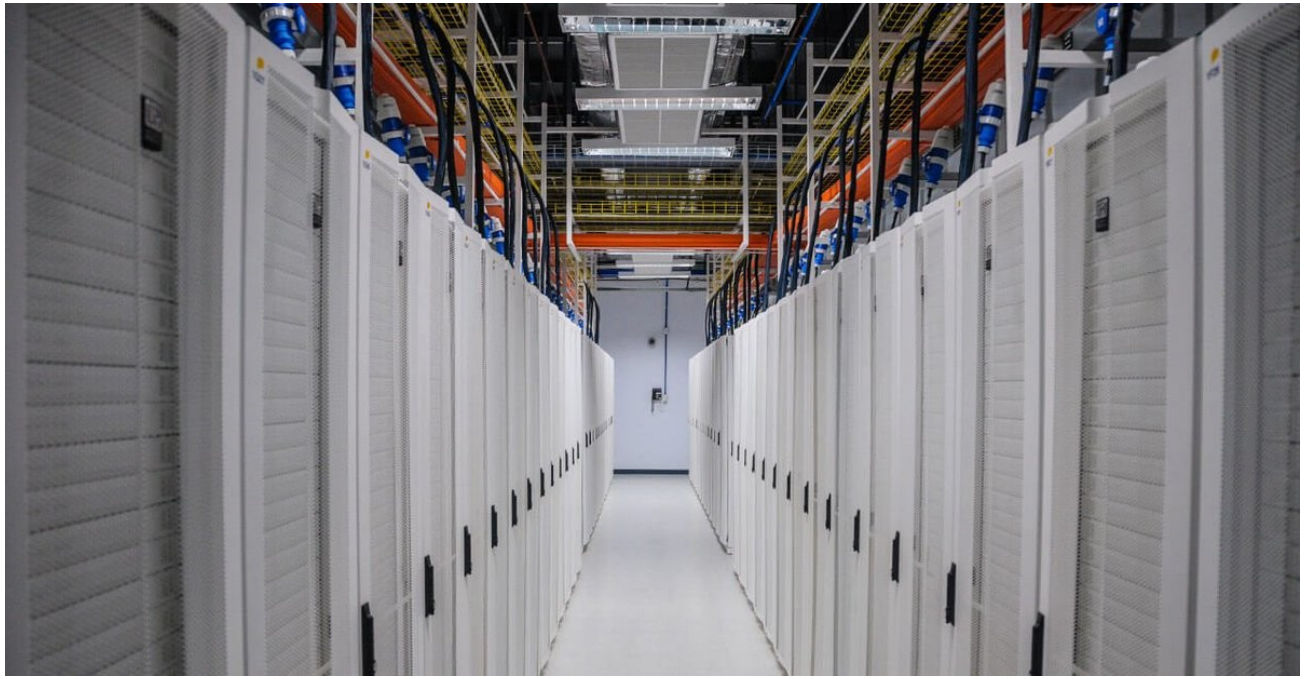
Networking en el datacenter

Facultad de Ingeniería – Universidad de la República

Datacenters

- Salas aclimatadas (refrigeración), fuentes de energía redundantes (esperemos), seguridad física…
- Muchos servidores. Y grandes necesidades de networking
- De todos los tamaños, aplicaciones muy heterogéneas
- Google/Facebook/Amazon/Microsoft: Datacenters con cientos de miles de servidores
  - Requerimientos importantes sobre la red de datacenter
- En muchos casos gran volumen de tráfico entre servidores (motores de búsqueda, servidores cloud, etc)

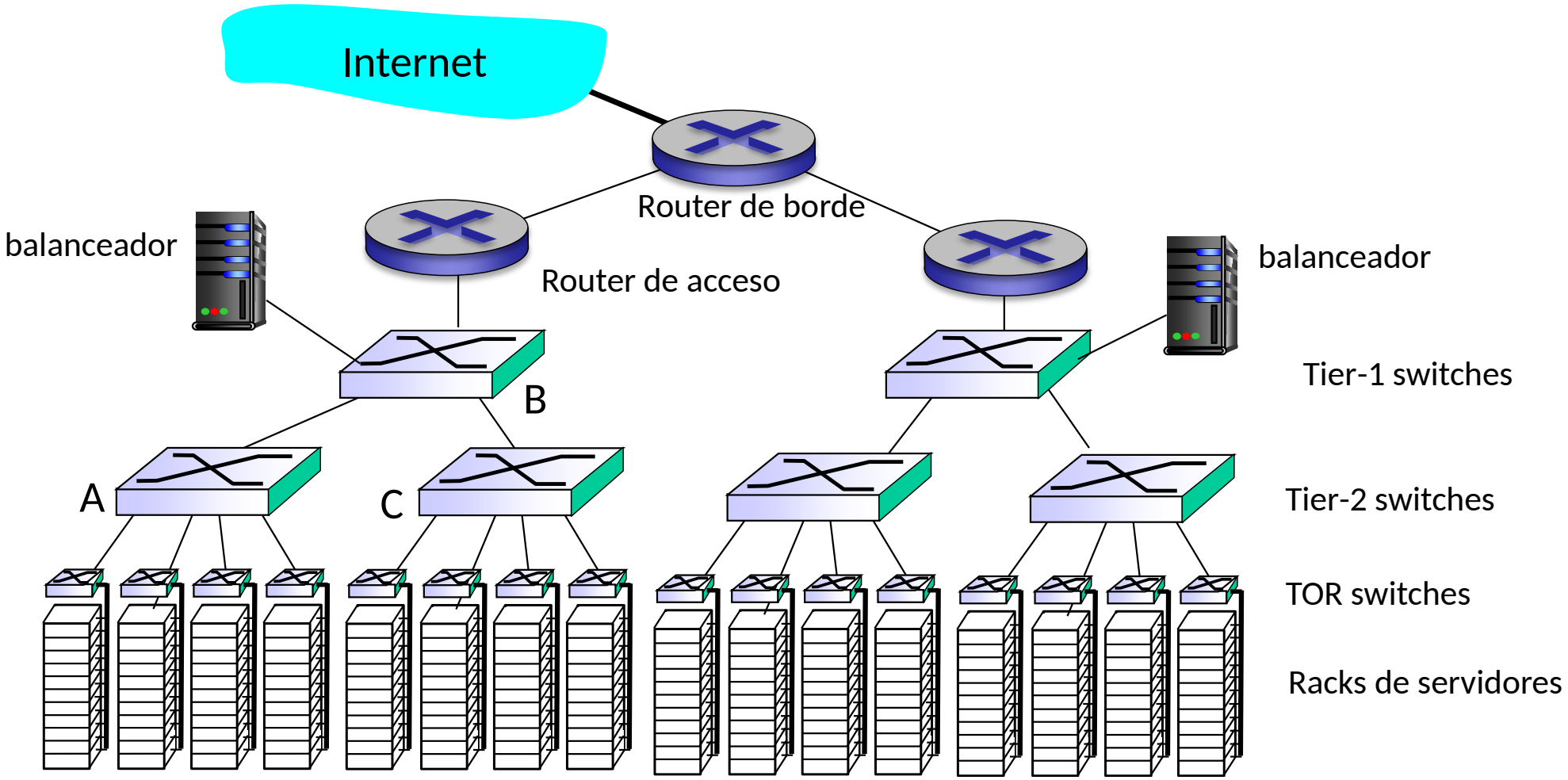
Ejemplo: datacenter de ANTEL



Fuente: página de ANTEL

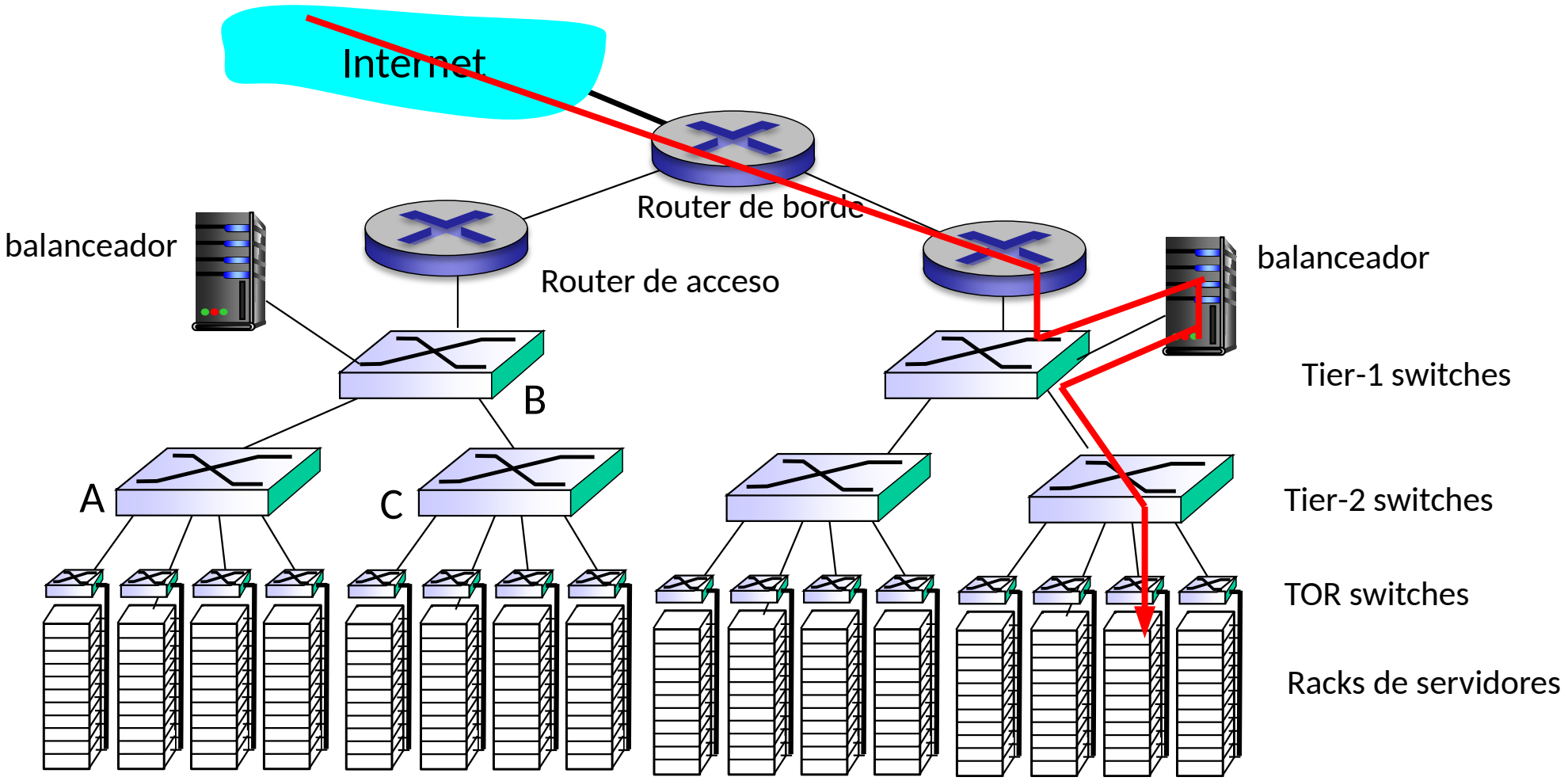
- De acuerdo a la información pública
  - 40.000 servidores
  - Más de 1000 racks
  - 12.000 m^2

Ejemplo: datacenter jerárquico



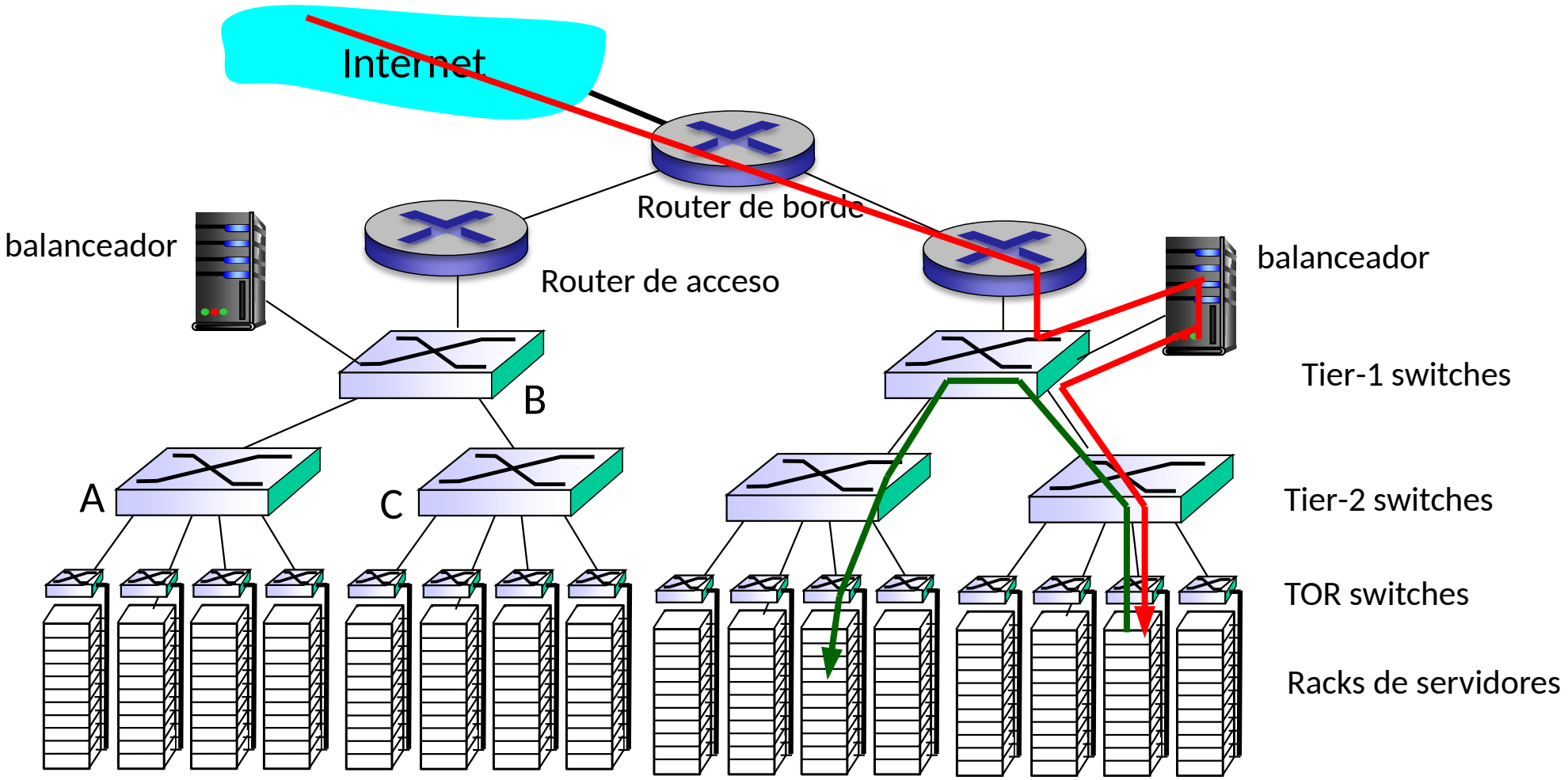
- Problema: si hay mucho tráfico entre servidores internos

Ejemplo: datacenter jerárquico



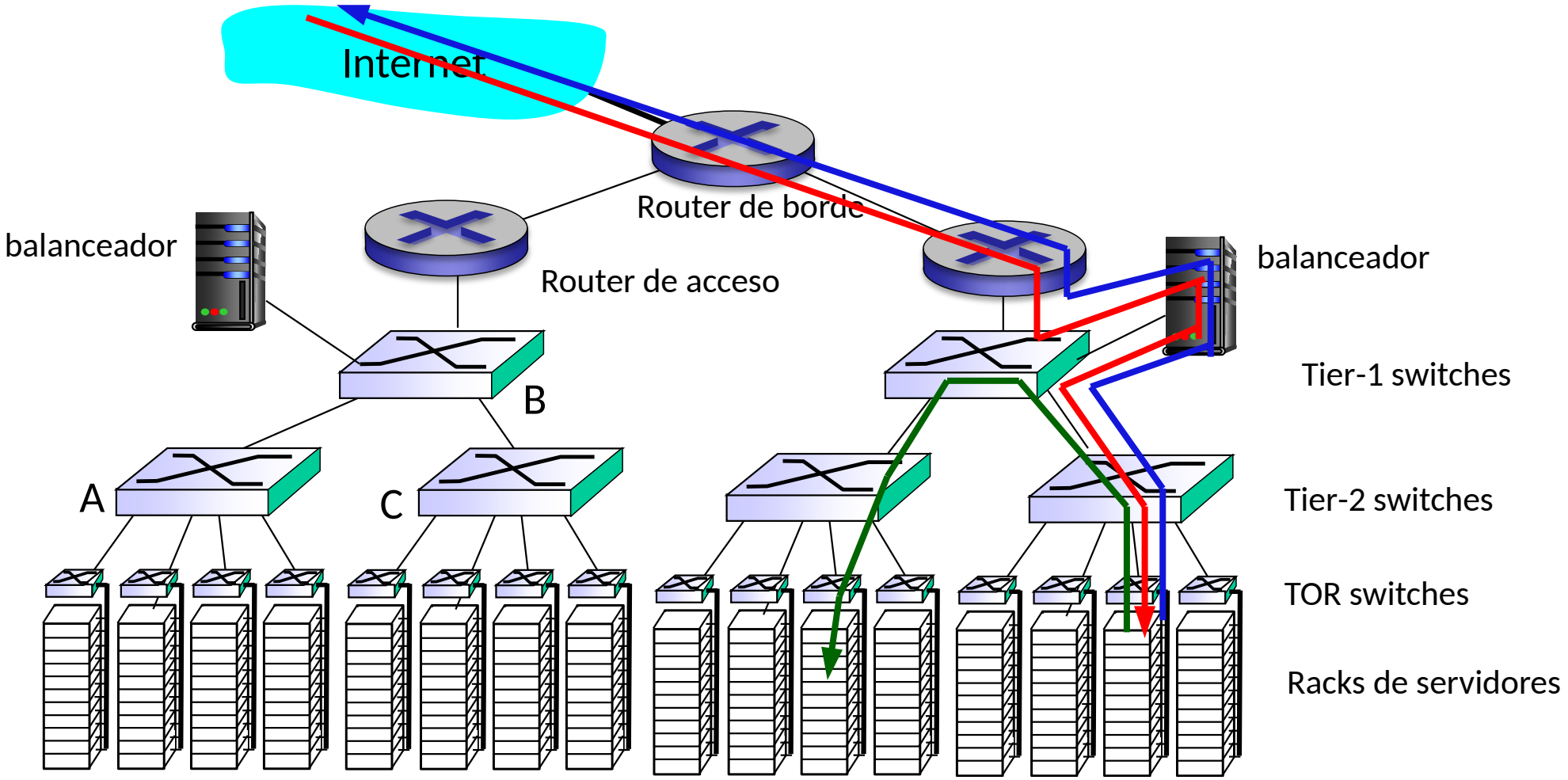
- Problema: si hay mucho tráfico entre servidores internos

Ejemplo: datacenter jerárquico



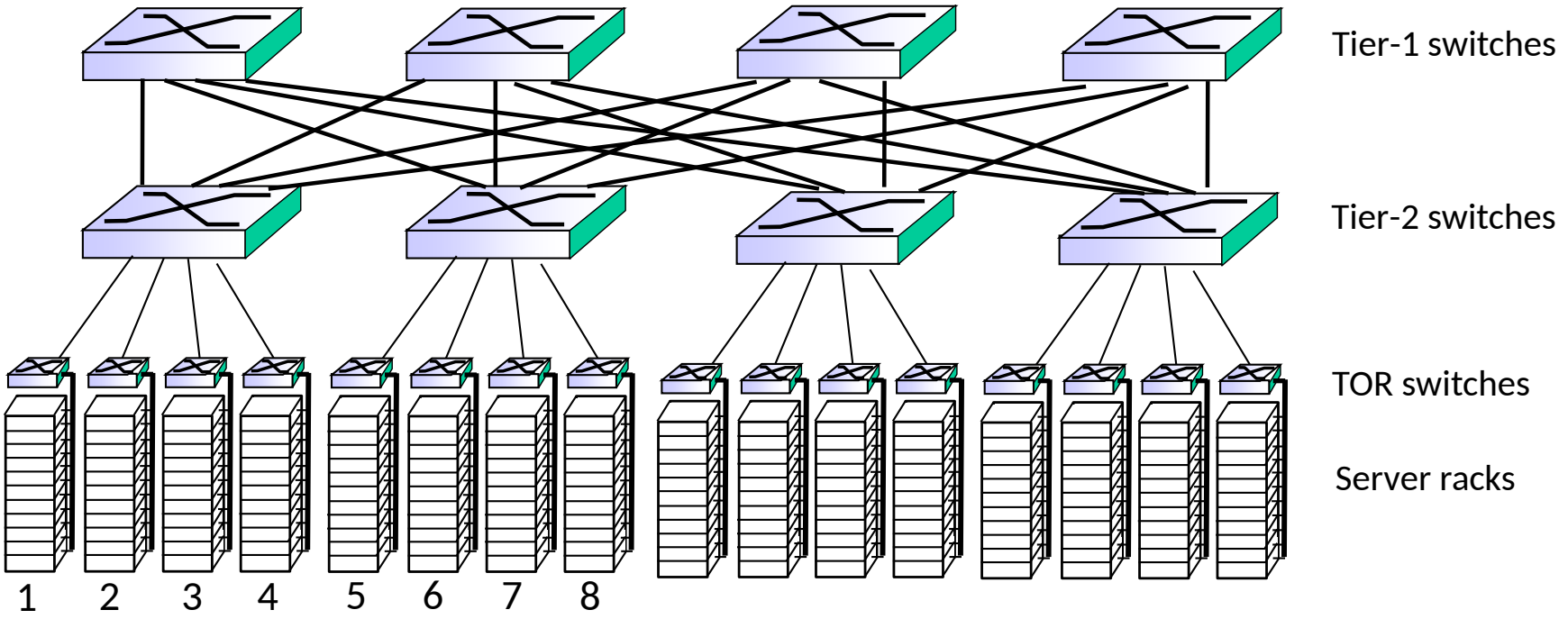
- Problema: si hay mucho tráfico entre servidores internos

Ejemplo: datacenter jerárquico



- Problema: si hay mucho tráfico entre servidores internos

Ejemplo: interconexión más densa



- Más capacidad entre racks (múltiples caminos posibles)
- Más redundancia