

Redes de datos 1

Redes de área local

Facultad de Ingeniería – Universidad de la República

Instituto de Ingeniería Eléctrica

2023

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

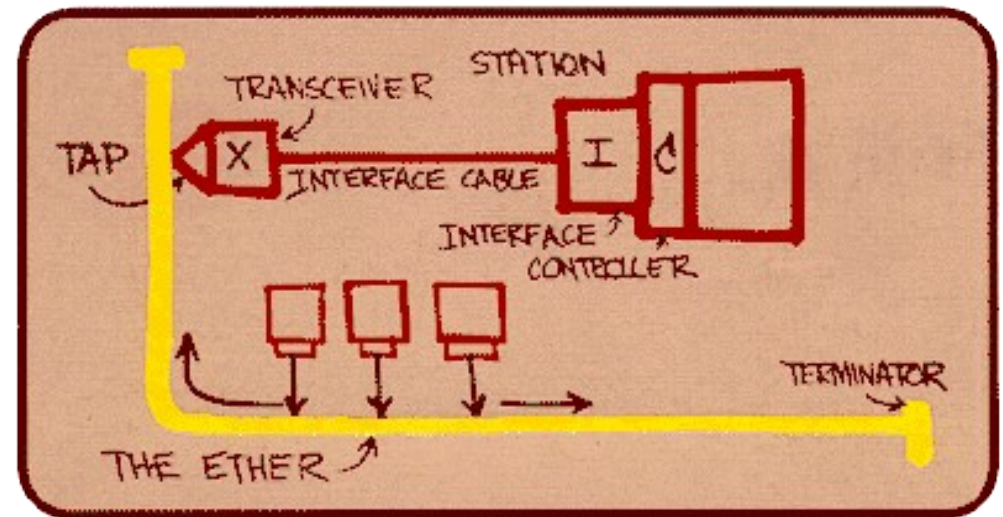
- Las primeras normas de la serie IEEE 802 surgieron a fines de la década de 1970 (802.1 a 802.5)
- 3 grandes grupos de interés, no pudieron conciliar una posición única
 - 3 normas incompatibles entre si
 - Dec, Intel, Xerox: 802.3 (Ethernet)
 - IBM: 802.5. Token Ring
 - General motors: 802.4. Token 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)

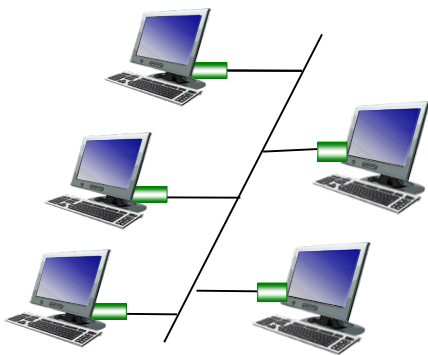
- Ethernet (IEEE 802.3) es el protocolo para redes de área local cableadas más utilizado hoy en día
- Su uso se ha extendido también a las redes de área amplia (WAN)
- Un conjunto de normas y actualizaciones a lo largo de 40 años
- Continúa evolucionando
- Primer versión: Bob Metcalfe y David Boggs (mediados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



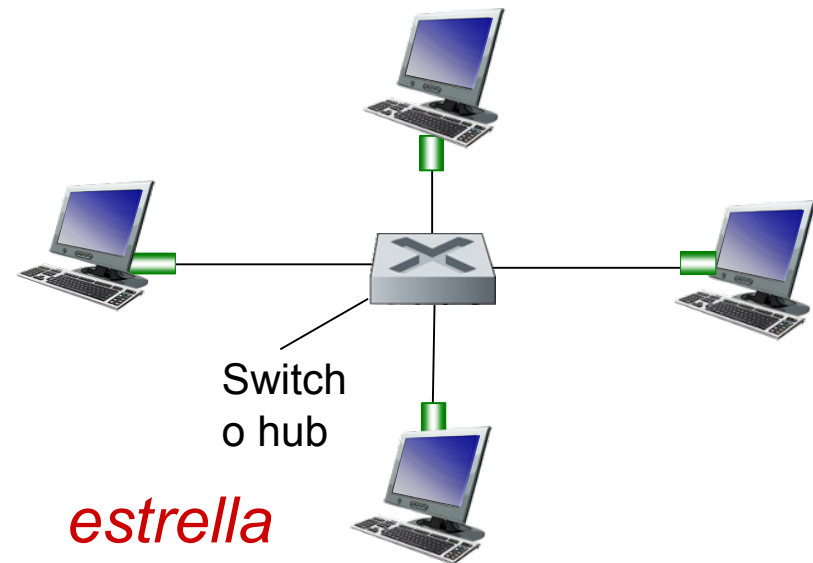
Sketch de la Ethernet de Bob Metcalfe

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 (p.e. Hub): 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 (grueso y delgado), fibra óptica, cable de par trenzado de cobre
 - 10base-5, 10base-2, 10base-F, 10base-T
- 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 2τ (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 $k \cdot (\text{tiempo de TX de 512 bits})$
- Máximo 0-1023
- 16 colisiones => reporto fracaso a capas superiores

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 diseñado para tener una tasa de errores muy baja (tasa de error de bit 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

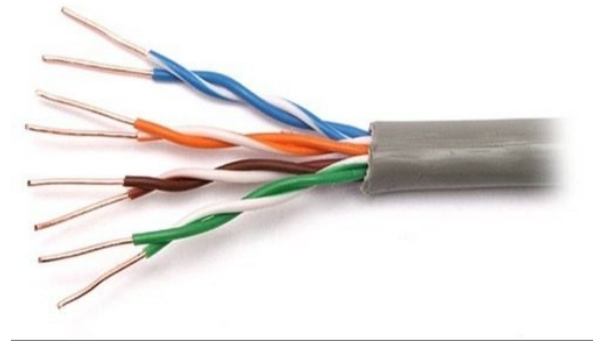
- “Fast Ethernet” (1995) IEEE 802.3u. 100 Mbps sobre cable de pares de cobre y sobre fibra
 - Sigue permitiéndose CSMA/CD, repetidores
 - Distancia máxima 100 metros al repetidor, máximo 1 repetidor
- Gigabit Ethernet (1998) IEEE 802.3z, 802.3ab. 1000 Mbps sobre fibra y cable de pares de cobre
 - Sigue permitiéndose CSMA/CD, repetidores (en la práctica solo se usan 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, 50 Gbps
- 200 Gbps y 400 Gbps (2017+)
- 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)
- En las conexiones en estrella, para la conexión al switch en la mayoría de los casos tenemos un canal para transmisión y uno para recepción
- 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

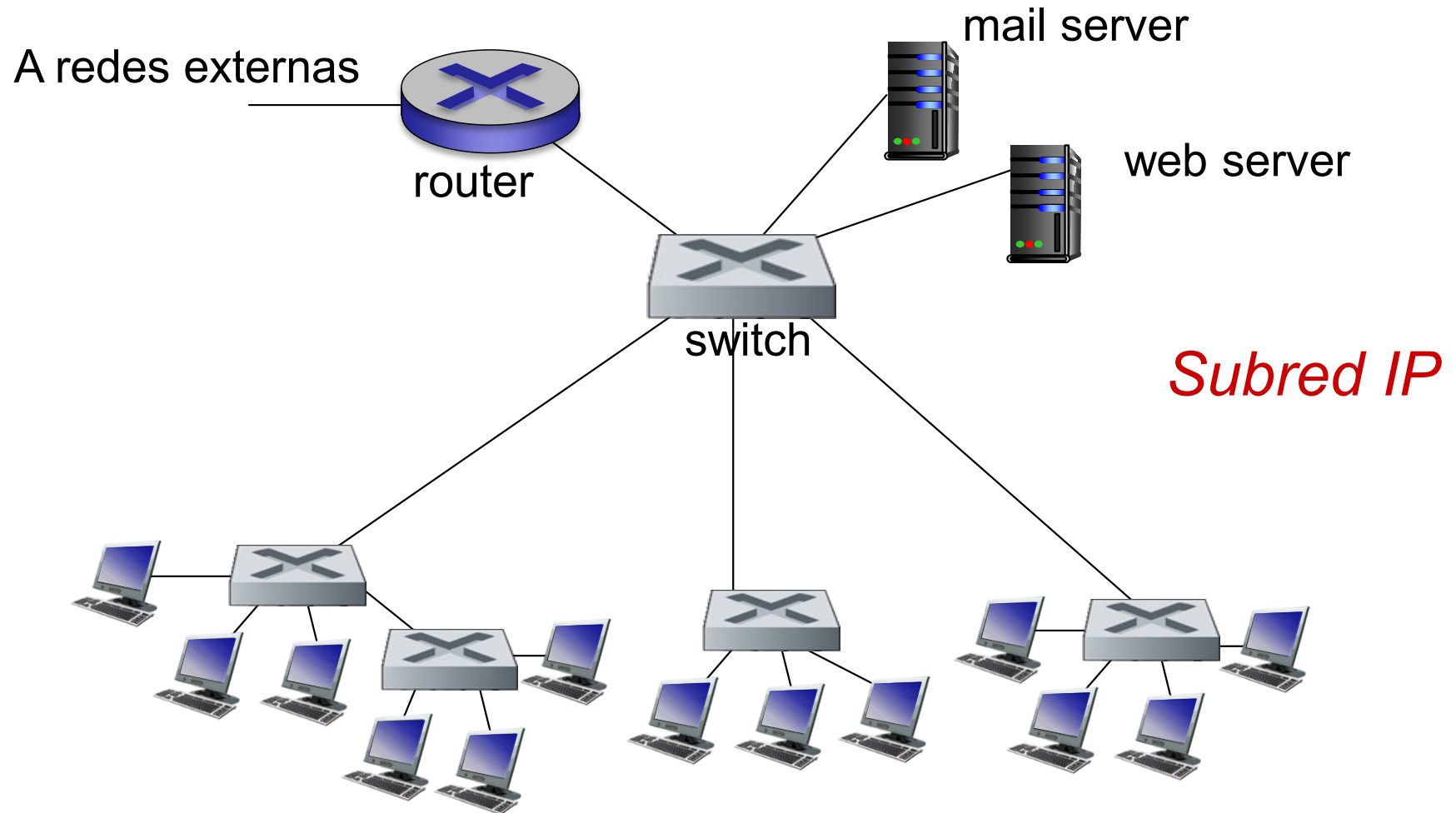
- Cable coaxial: solo en 802.3 a 10 Mbps (obsoleto)
- Par trenzado: 4 pares de alambres de cobre
 - Categoría 3: 10 Mbps
 - Categoría 5: 100 Mbps
 - Categoría 5e, 6: 1 Gbps
 - Categoría 7, 8: 10 Gbps (cables armados)
- Otros cables de cobre armados: 40 Gbps, 100Gbps+
- Fibra óptica: todas las velocidades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



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 hosts no notan la presencia de un switch
- Son “plug and play”. No requieren configuración, aprenden de forma autónoma

Ejemplo de red con switches

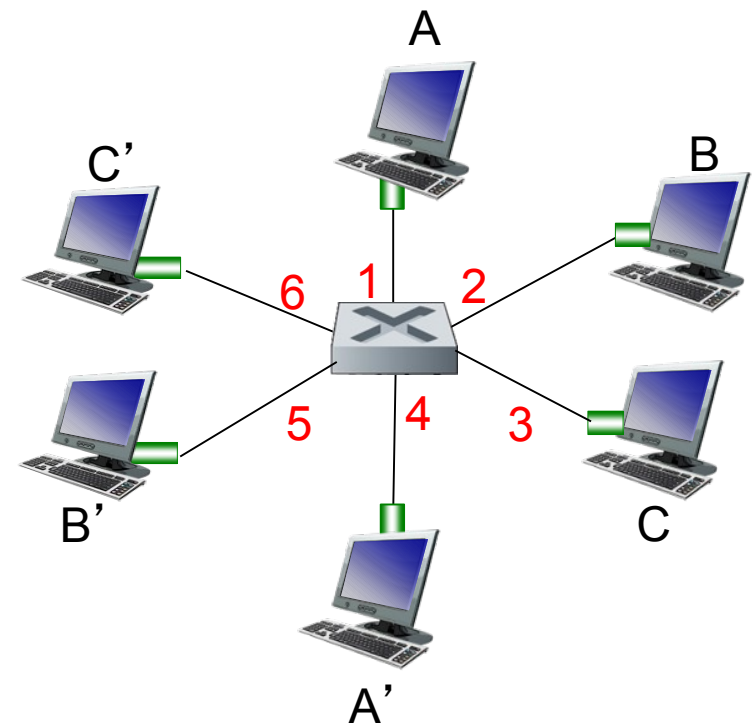


Funcionamiento de un switch

- 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 de forma continua



*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

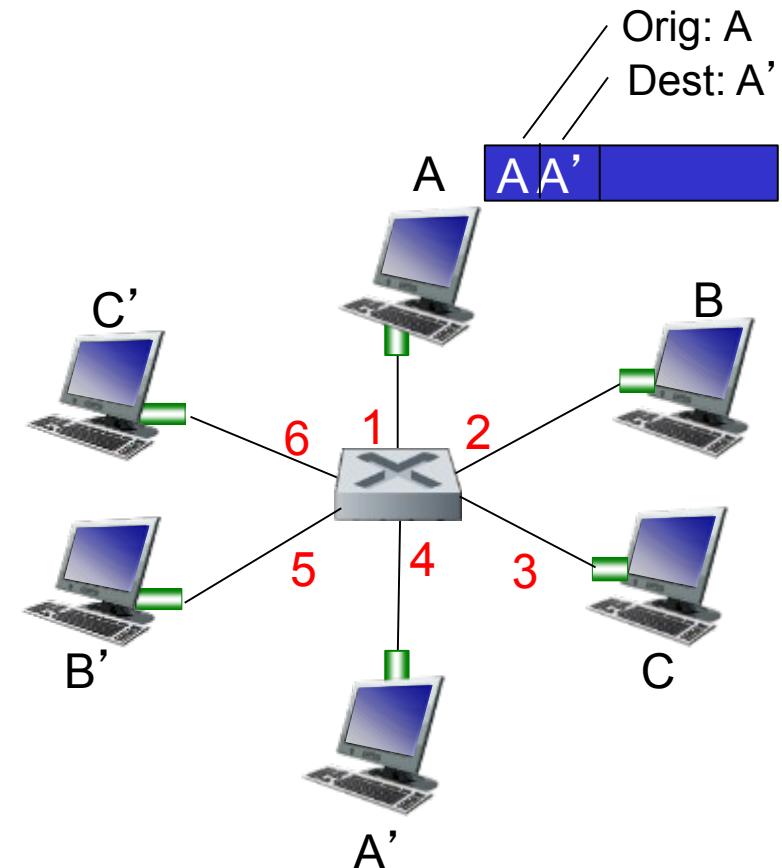
| Dirección MAC | Puerto | Tiempo |
|-------------------|--------|--------|
| 62:FE:F7:11:89:A3 | 3 | 9:32 |
| 7C:BA:11:E1:55:A1 | 4 | 2:40 |
| | ... | |

- Direcciones Broadcast: Se reenvía por todos los puertos (inundación)
- 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?
- Cuando A envía una trama a A'
 - switch recibe trama
 - Observa dirección DE ORIGEN (A)
 - Agrega entrada en tabla para A

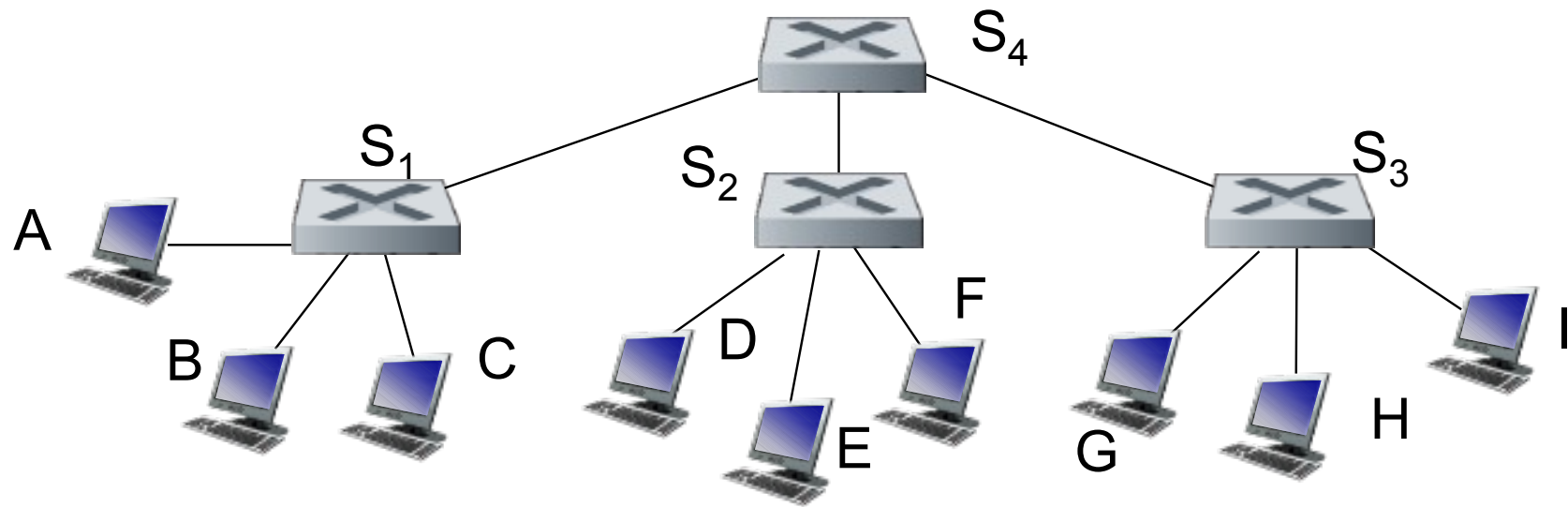
| Dirección MAC | Puerto | TTL |
|---------------|--------|-------|
| A | 1 | 20:00 |
| ... | ... | ... |



Filtrado y forwarding

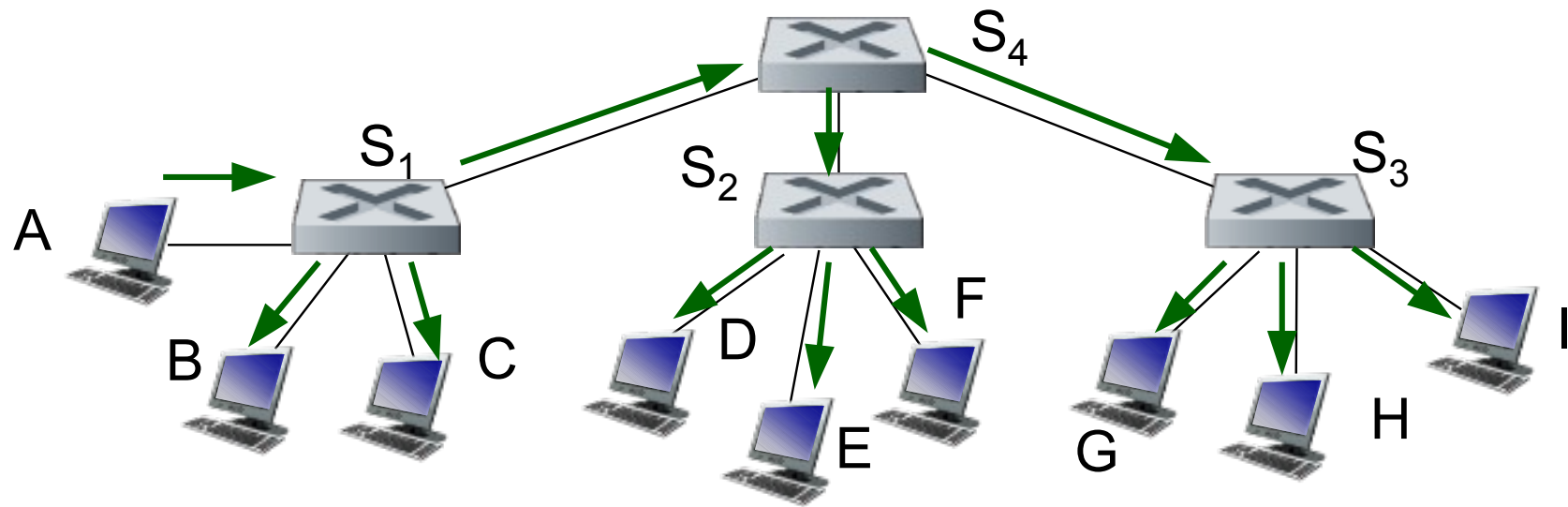
- Cuando el switch recibe una trama:
 - 1) Guardar o actualizar entrada para la dirección MAC de origen
 - 2) Si dirección de destino es broadcast → Inundar
 - 3) Si dirección de destino es multicast → actuar de acuerdo a configuración (por defecto se inunda)
 - 4) Buscar dirección de destino en la tabla
 - 5) Si no se encontró en la tabla → Inundar
 - 6) 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



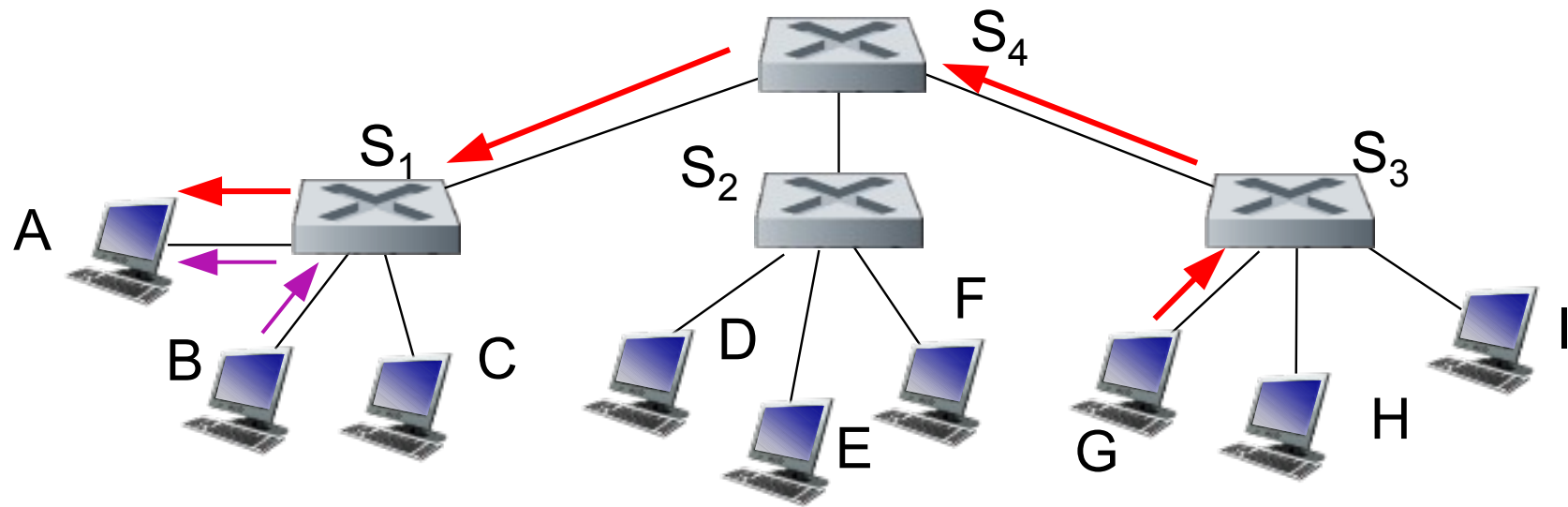
- Tablas inicialmente vacías

Ejemplo



- A envía trama a B:
 - 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

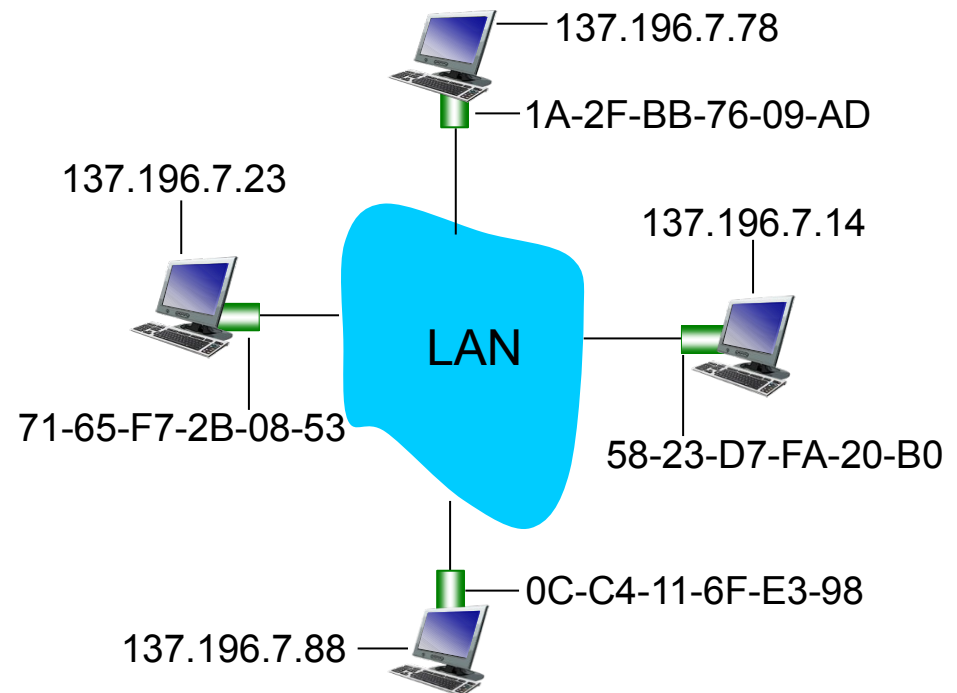
Ejemplo (cont.)



- 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

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 |
| | | |

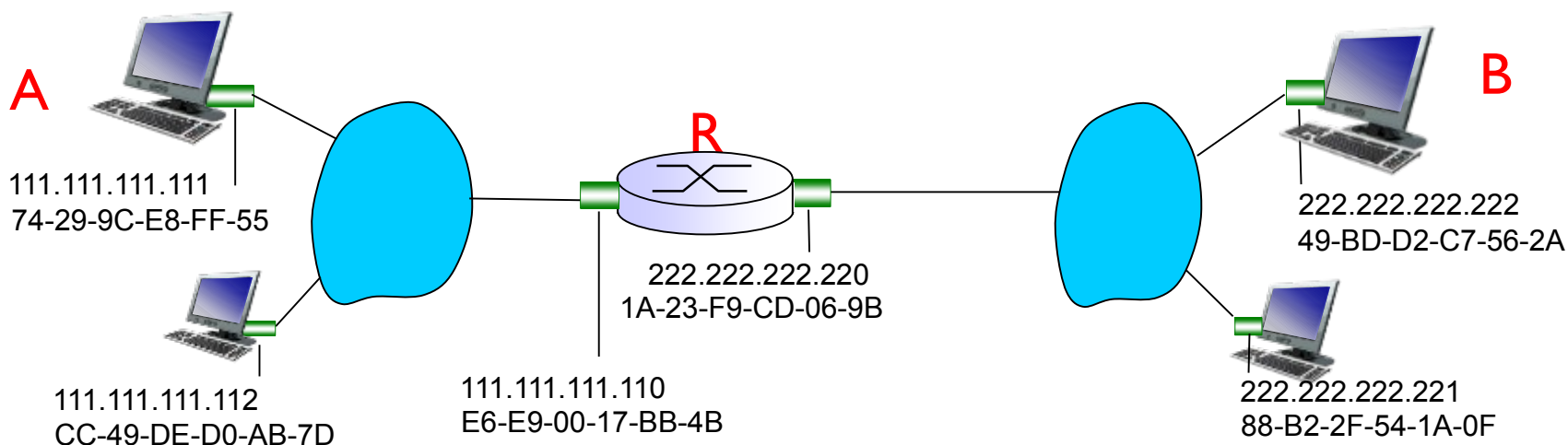
- Solamente tendremos entradas en la tabla para las IPs con las que intercambiamos tráfico
- El tiempo de vida permite borrar las entradas (o refrescarlas si están en uso) luego de un tiempo prudencial (minutos)
- Observar que esta tabla NO está relacionada con la tabla de un switch
- ¿quiénes tienen una tabla de ARP? Los dispositivos que disponen de una capa 3 (enrutadores y hosts)

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 (trama con respuesta ARP)
 - 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

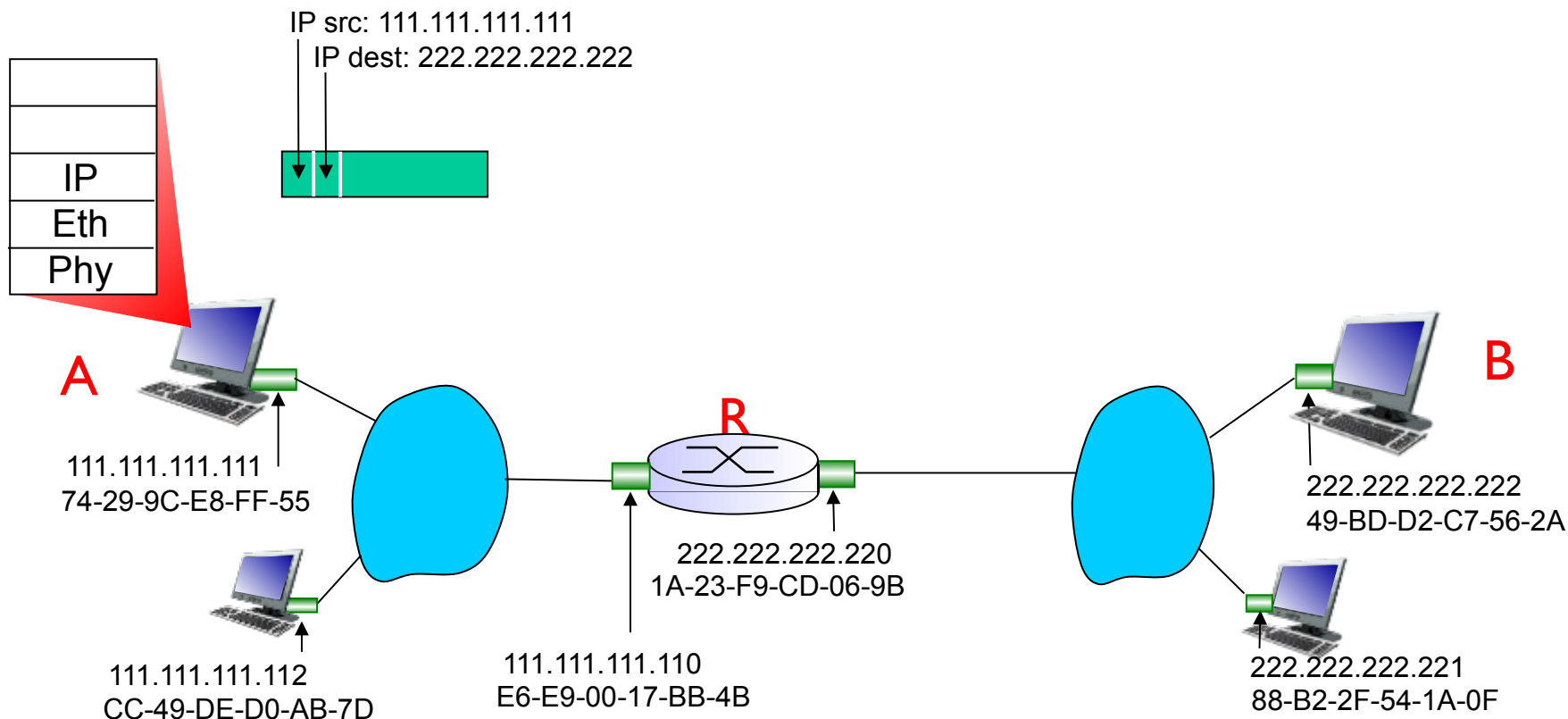
Ejemplo: enrutamiento hacia otra LAN

- 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



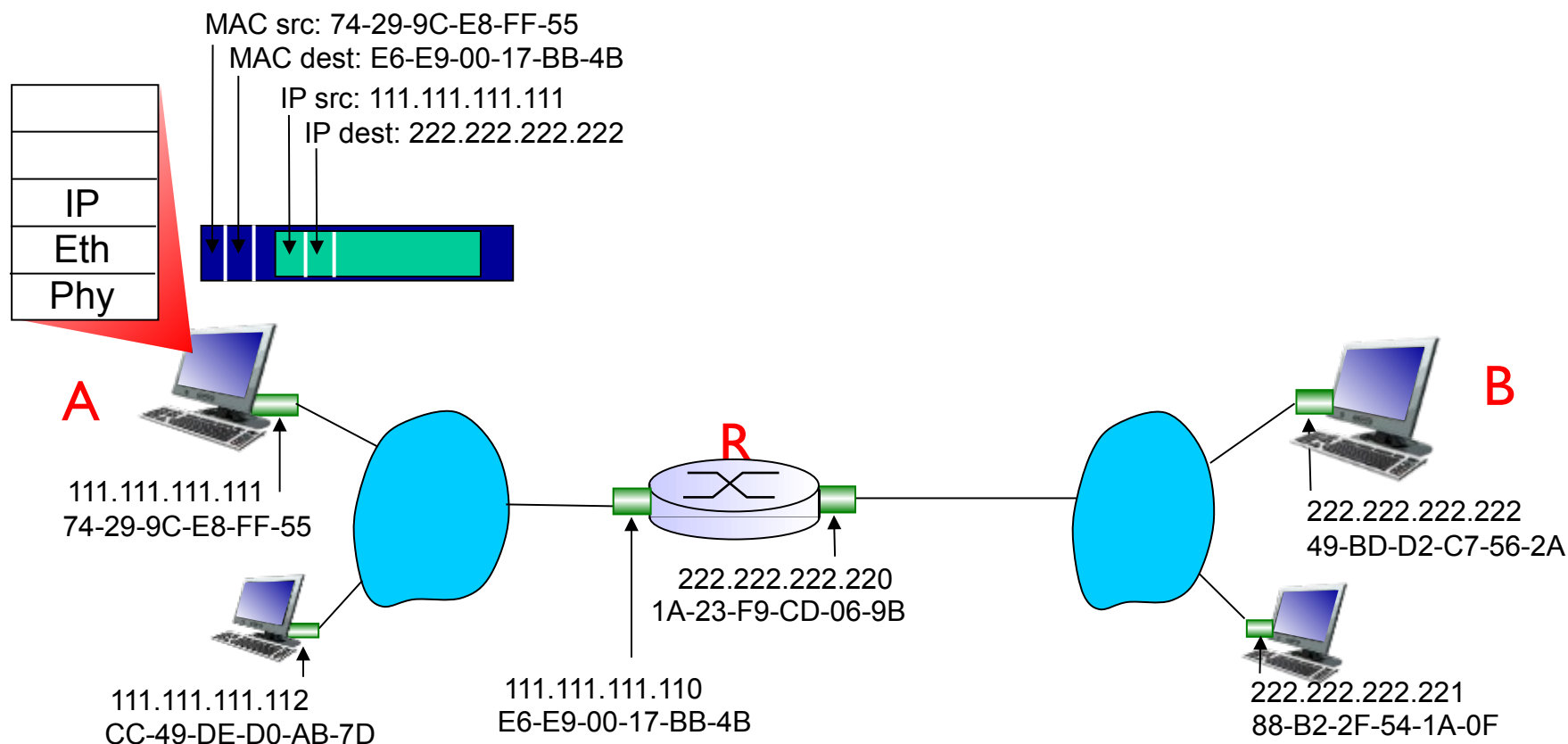
Ejemplo: enrutamiento hacia otra LAN (cont)

- 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



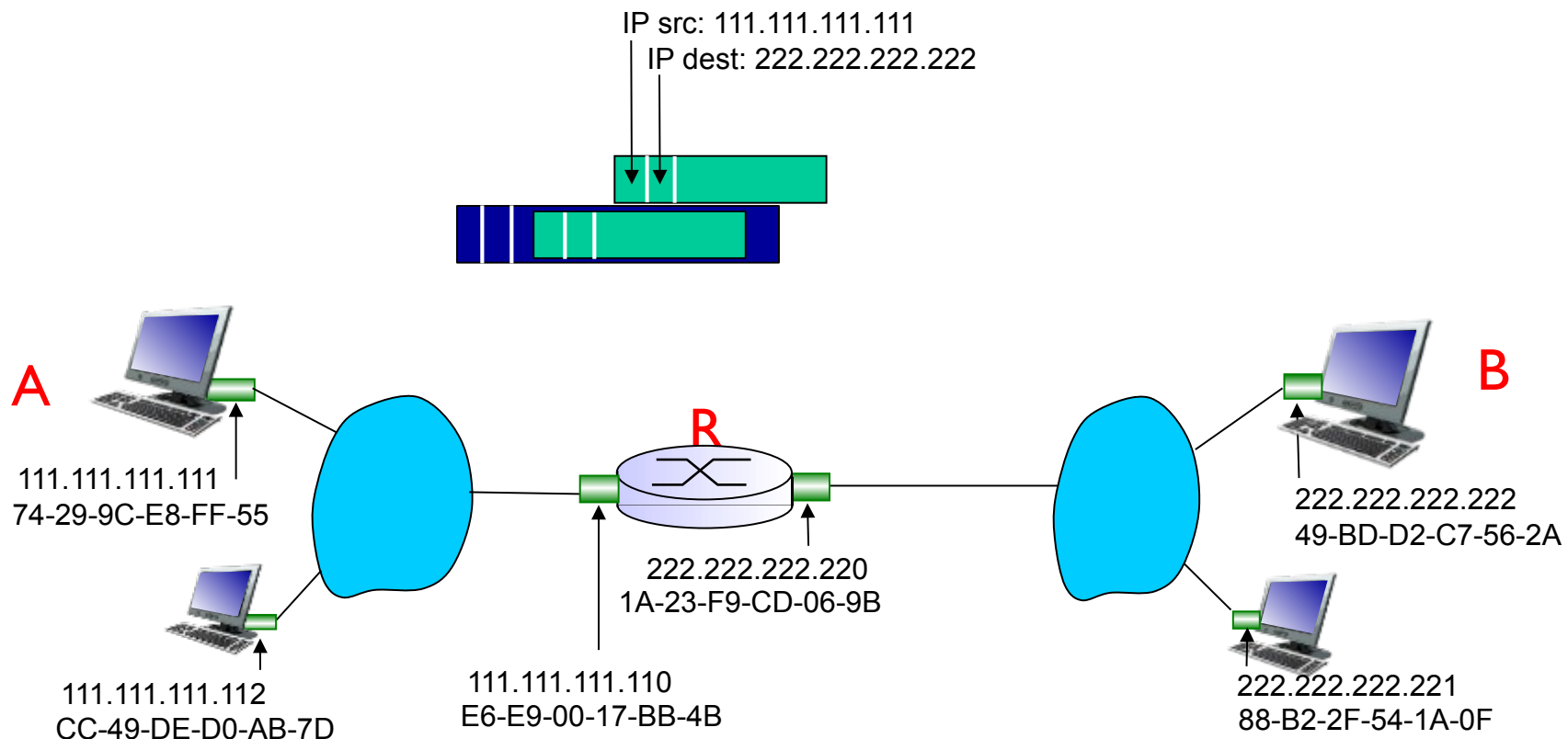
Ejemplo: enrutamiento hacia otra LAN (cont)

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



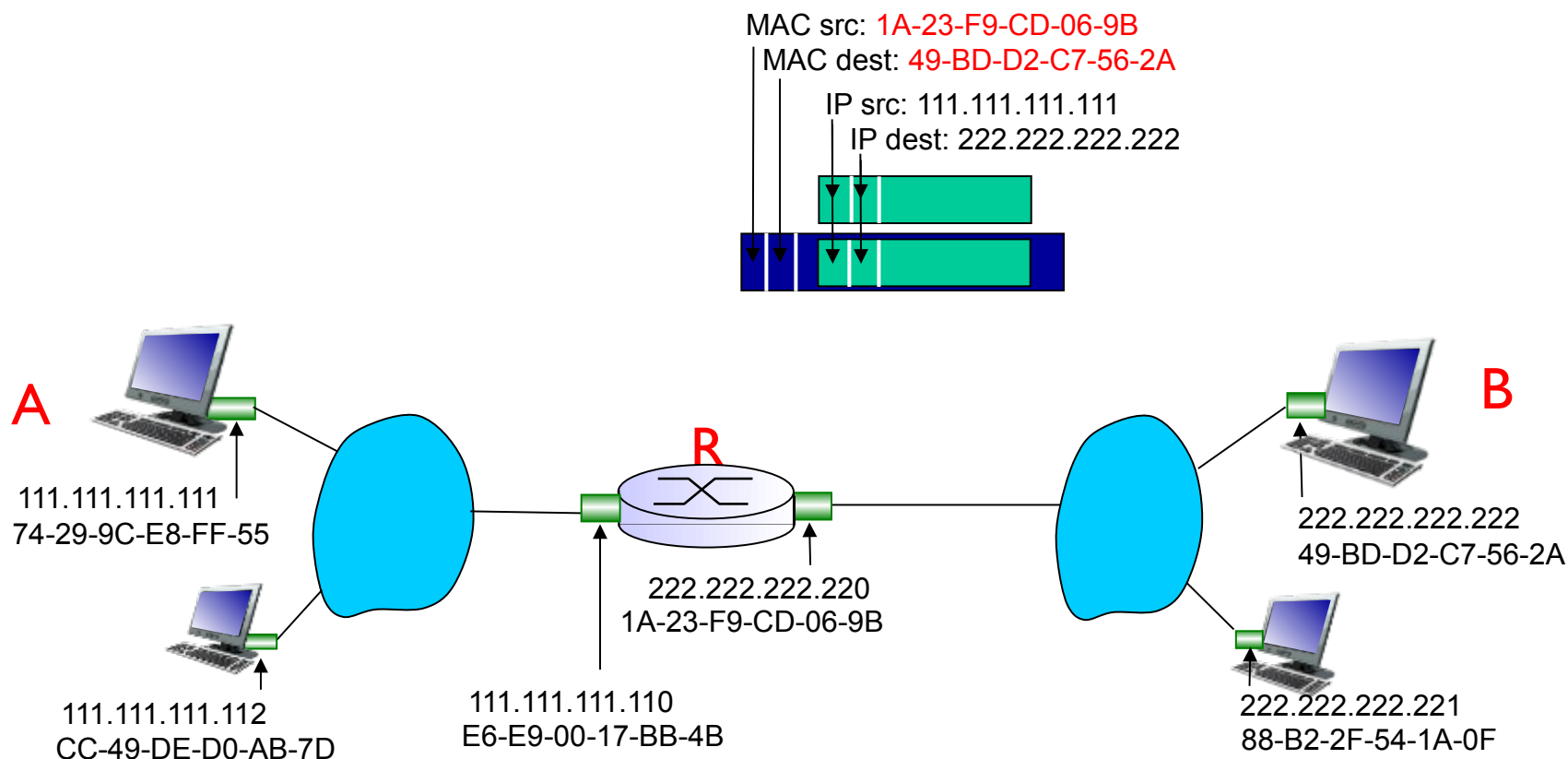
Ejemplo: enrutamiento hacia otra LAN (cont)

- 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



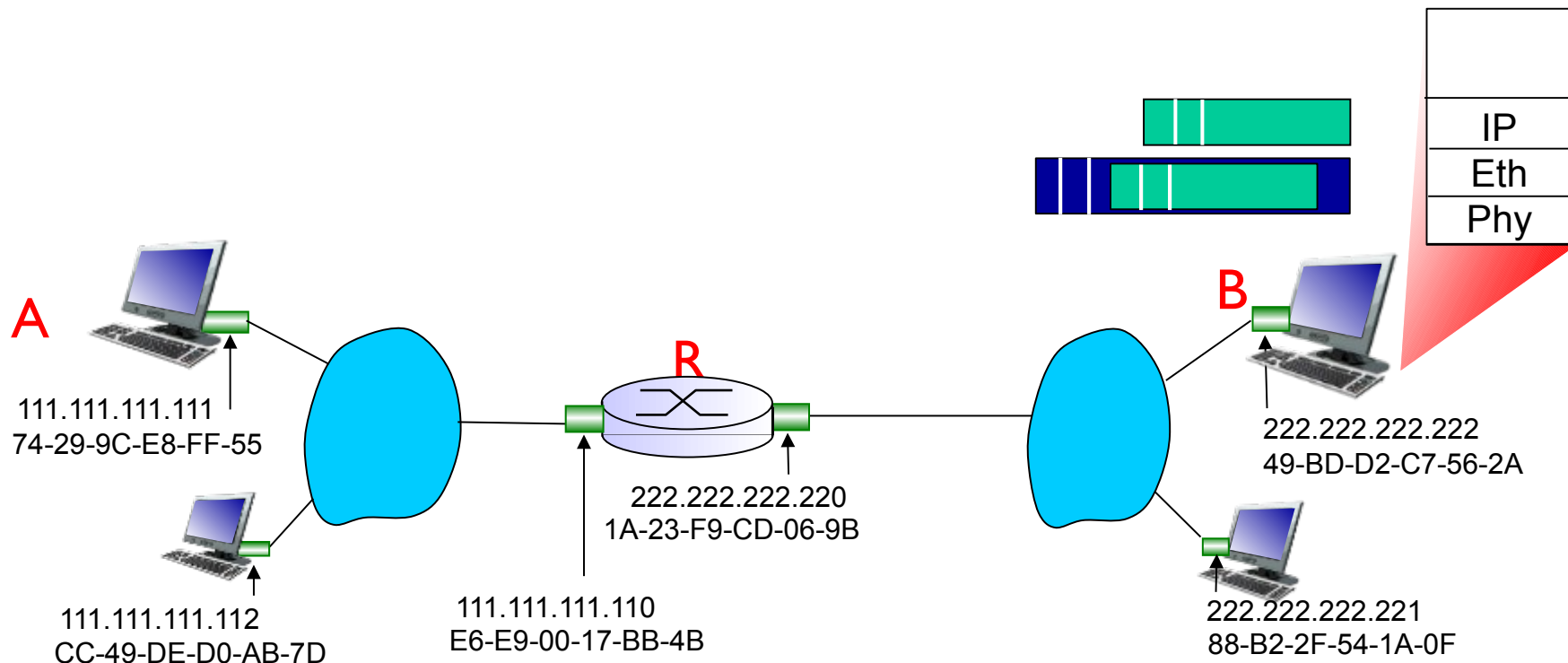
Ejemplo: enrutamiento hacia otra LAN (cont)

- R 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



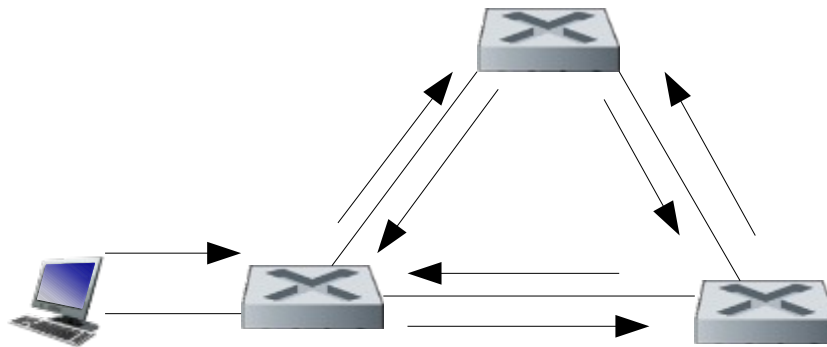
Ejemplo: enrutamiento hacia otra LAN (cont)

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



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

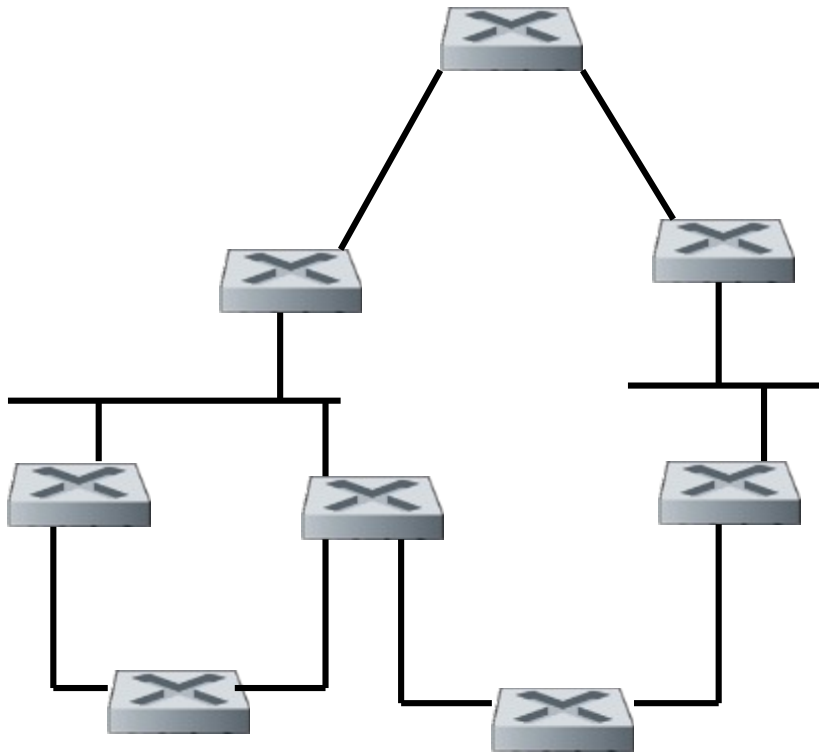


Spanning tree (802.1D)

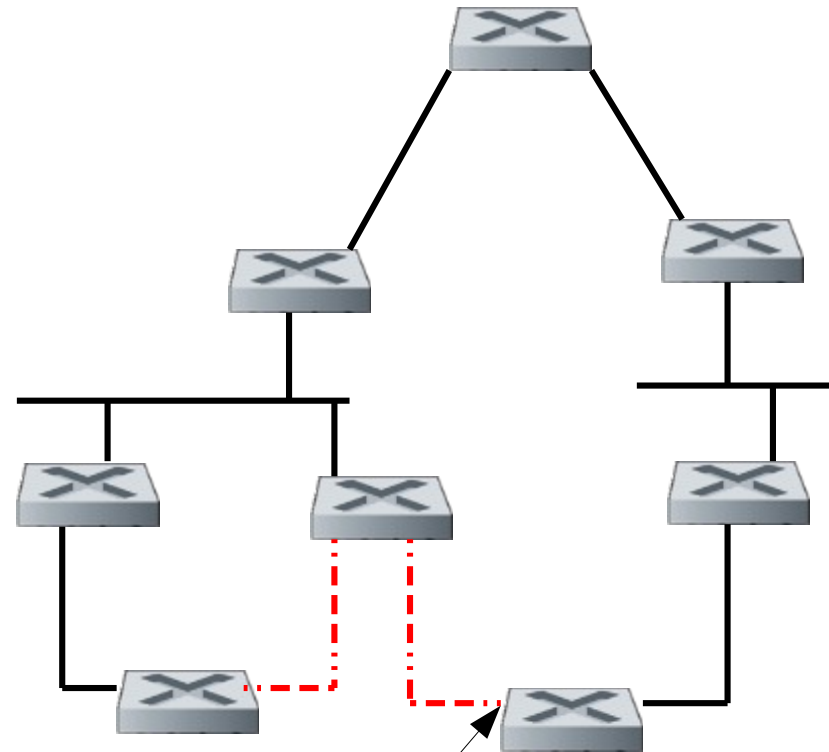
- Solución tradicional para evitar los loops
- Protocolo de capa de enlace entre switches
- Originalmente 802.1D.
 - Rapid Spanning Tree: 802.1w
 - Multiple Spanning Tree: 802.1s
- Construye un árbol sin loops bloqueando los links redundantes
 - Se elige un switch como raíz
 - Desde la raíz se van eligiendo 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

Ejemplo: topología y spanning tree

Topología Física



Spanning Tree



- 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

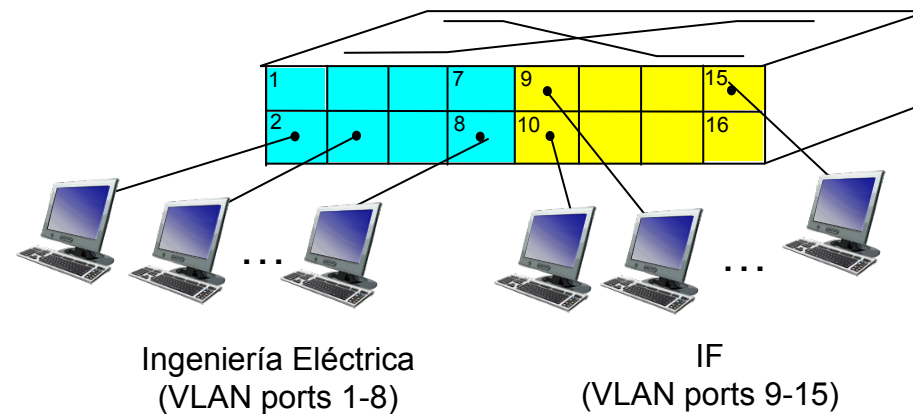
Virtual Local Area Networks (VLANs)

- 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

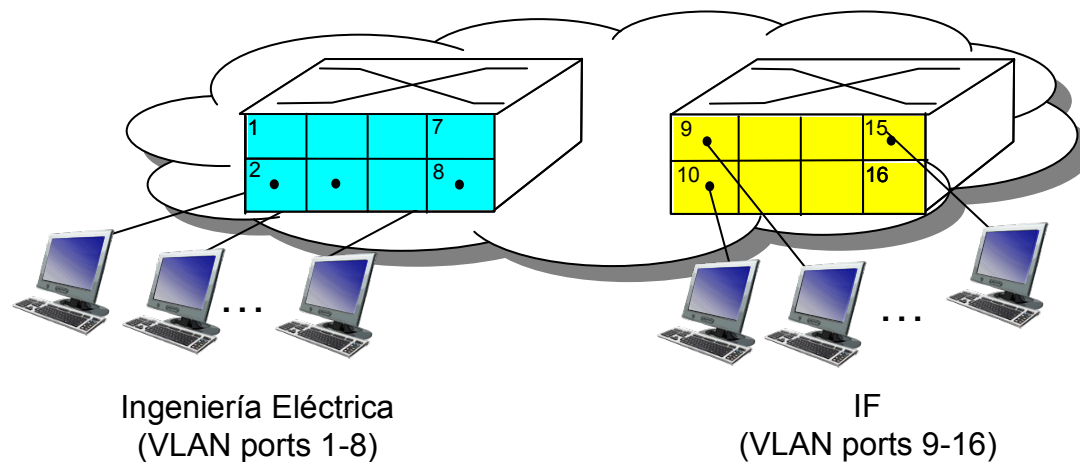
VLANs

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

Estructura física

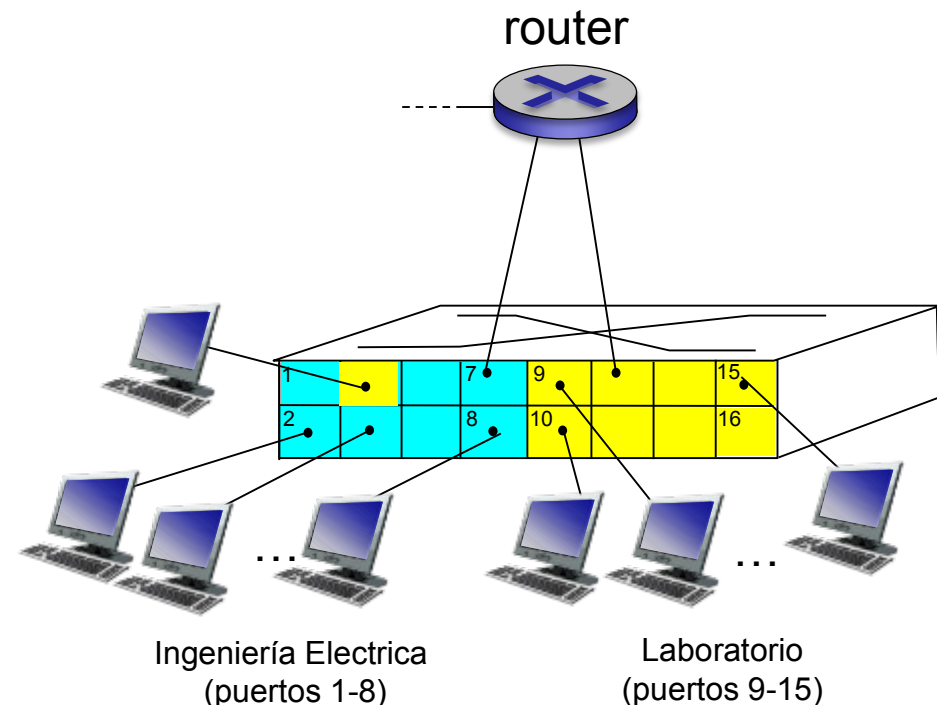


Estructura lógica



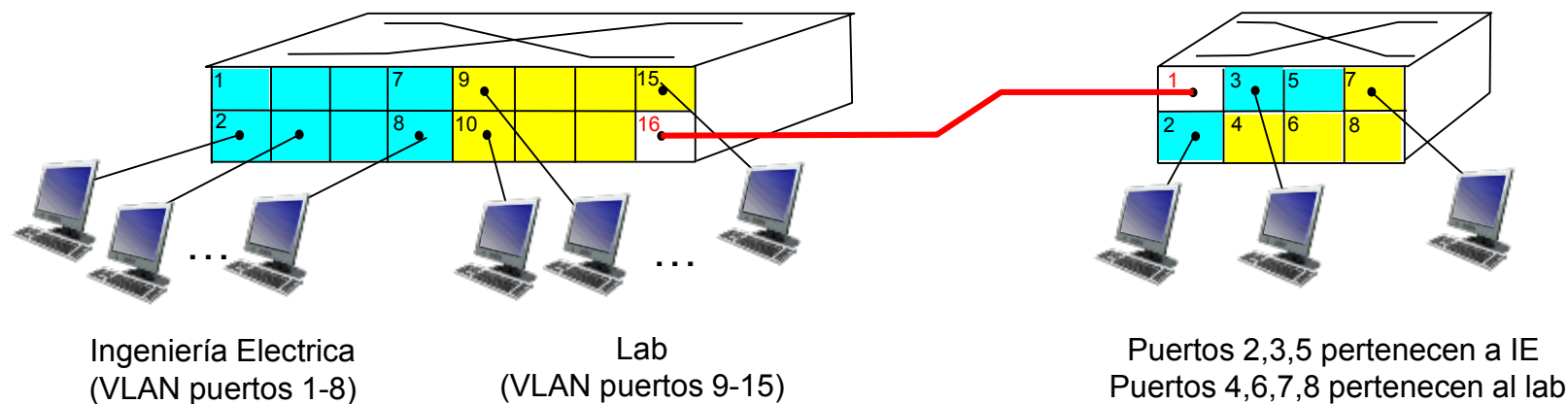
Ventajas de utilizar VLANs

- 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
- Interconexión entre vlans:
 - Router



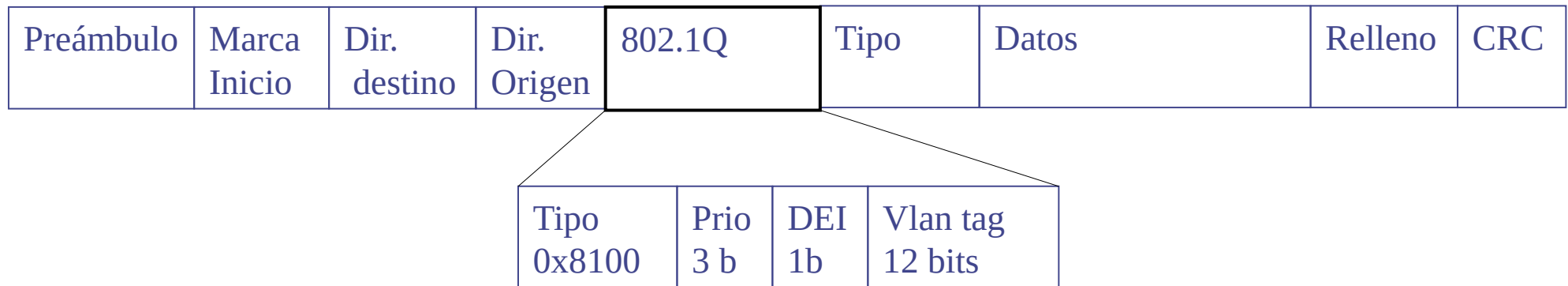
Vlans entre distintos switches

- ¿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



802.1Q

| | | | | | | | |
|-----------|--------------|--------------|-------------|------|-------|---------|-----|
| Preámbulo | Marca Inicio | Dir. destino | Dir. Origen | Tipo | Datos | Relleno | CRC |
|-----------|--------------|--------------|-------------|------|-------|---------|-----|



- Se insertan 4 bytes en 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

Networking en el datacenter

Facultad de Ingeniería – Universidad de la República
Instituto de Ingeniería Eléctrica

Datacenters

- Salas climatizadas (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)

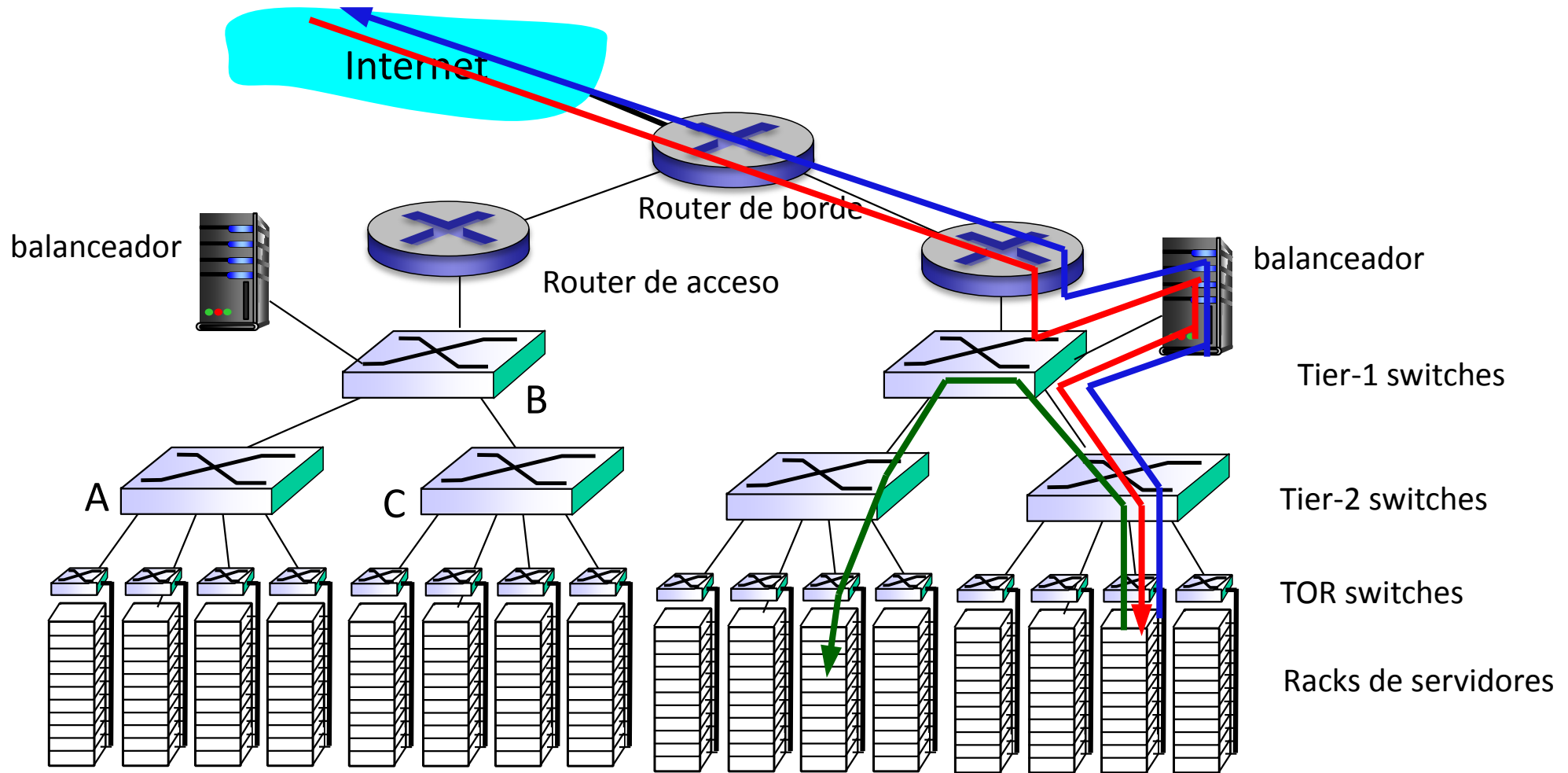
Ejemplo: datacenter de ANTEL



Fuente: página web de ANTEL (2019)

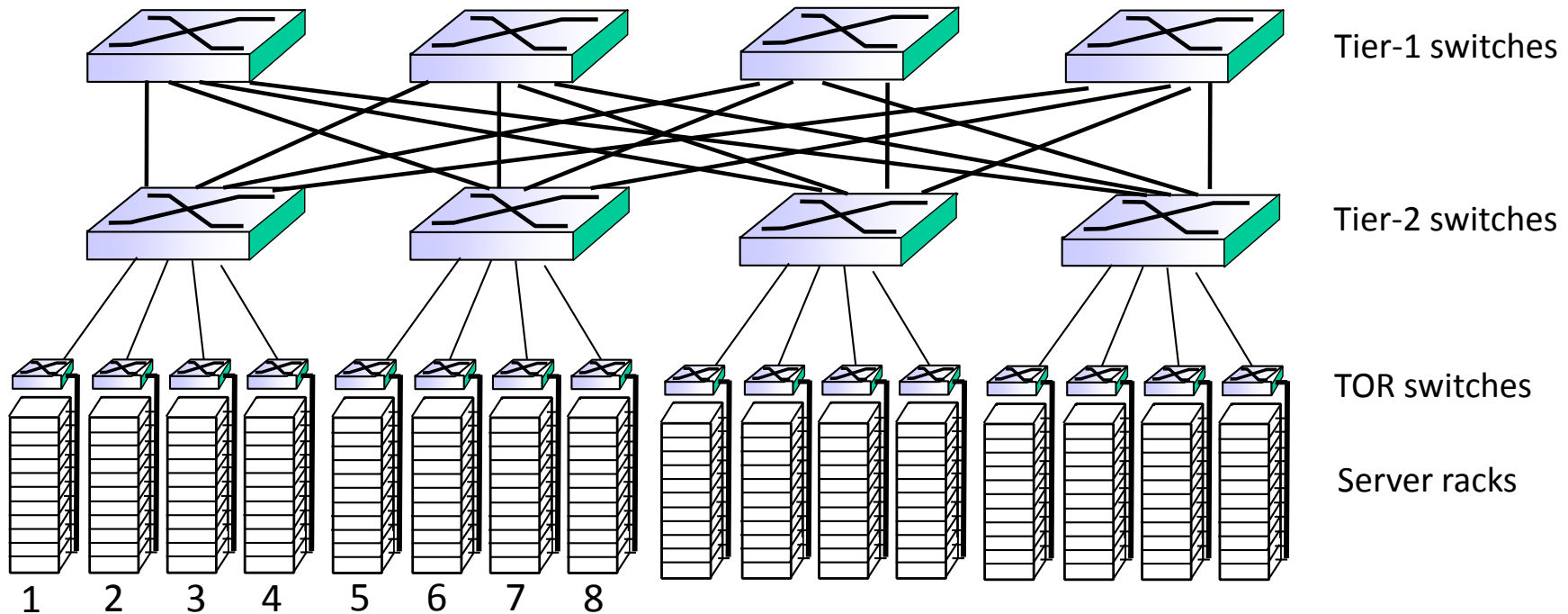
- De acuerdo a la información pública
 - 40.000 servidores
 - Más de 1000 racks
 - 12.000 m²

Ejemplo: datacenter jerárquico



- Problema: ¿qué pasa si hay mucho tráfico entre servidores internos?

Ejemplo: interconexión más densa



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

Redes de datos 1

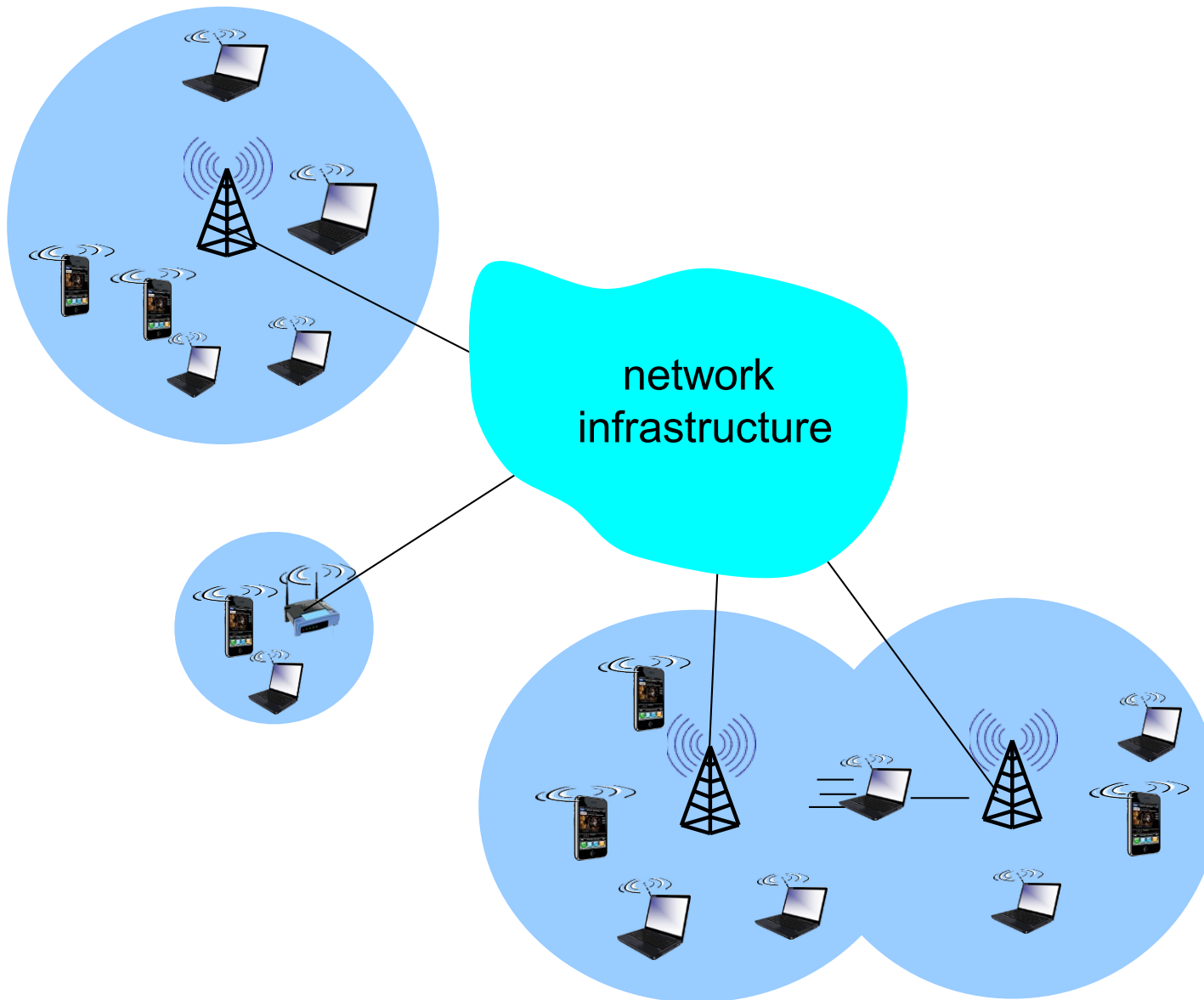
Redes inalámbricas

Facultad de Ingeniería – Universidad de la República
Instituto de Ingeniería Eléctrica

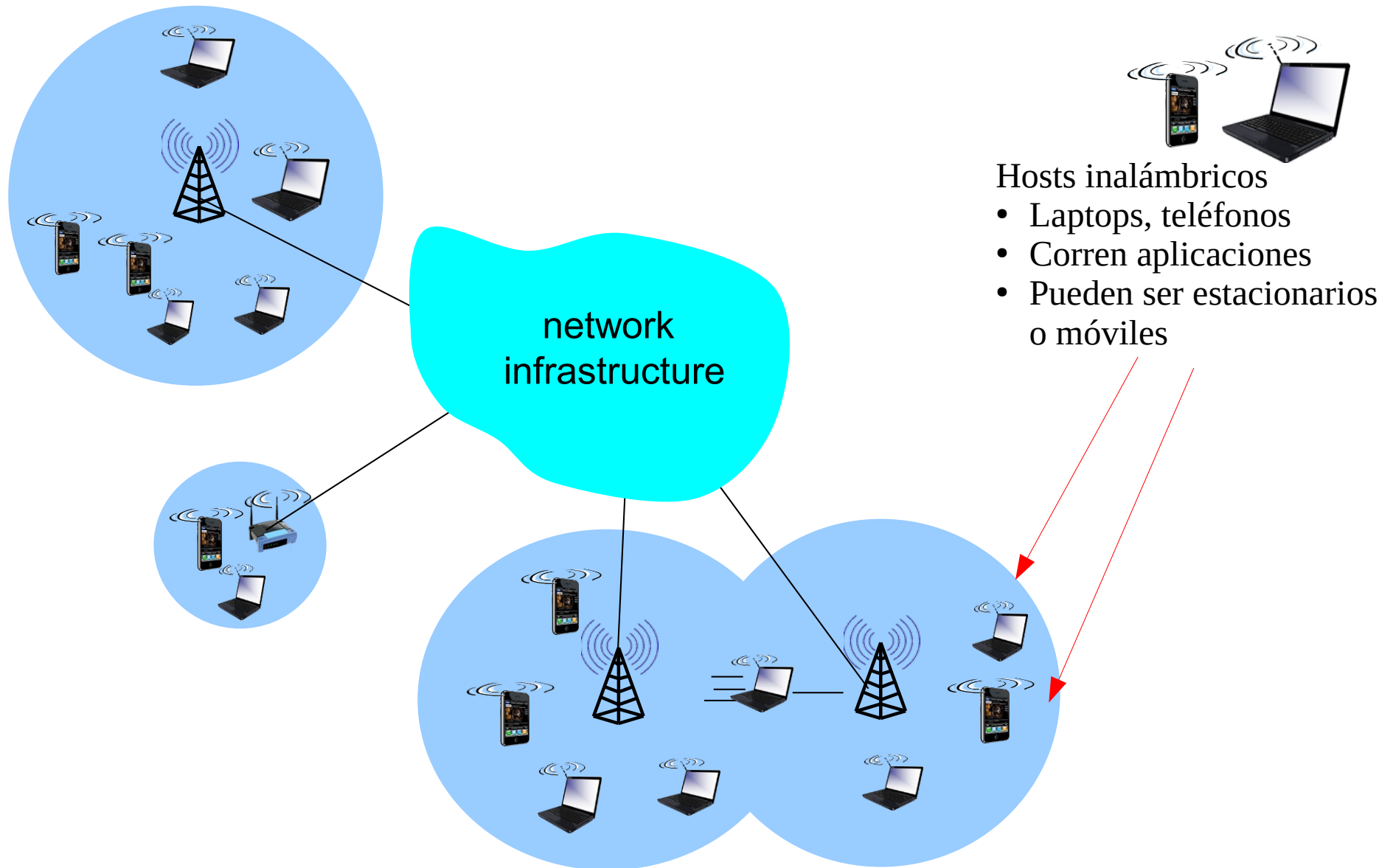
Redes inalámbricas

- 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

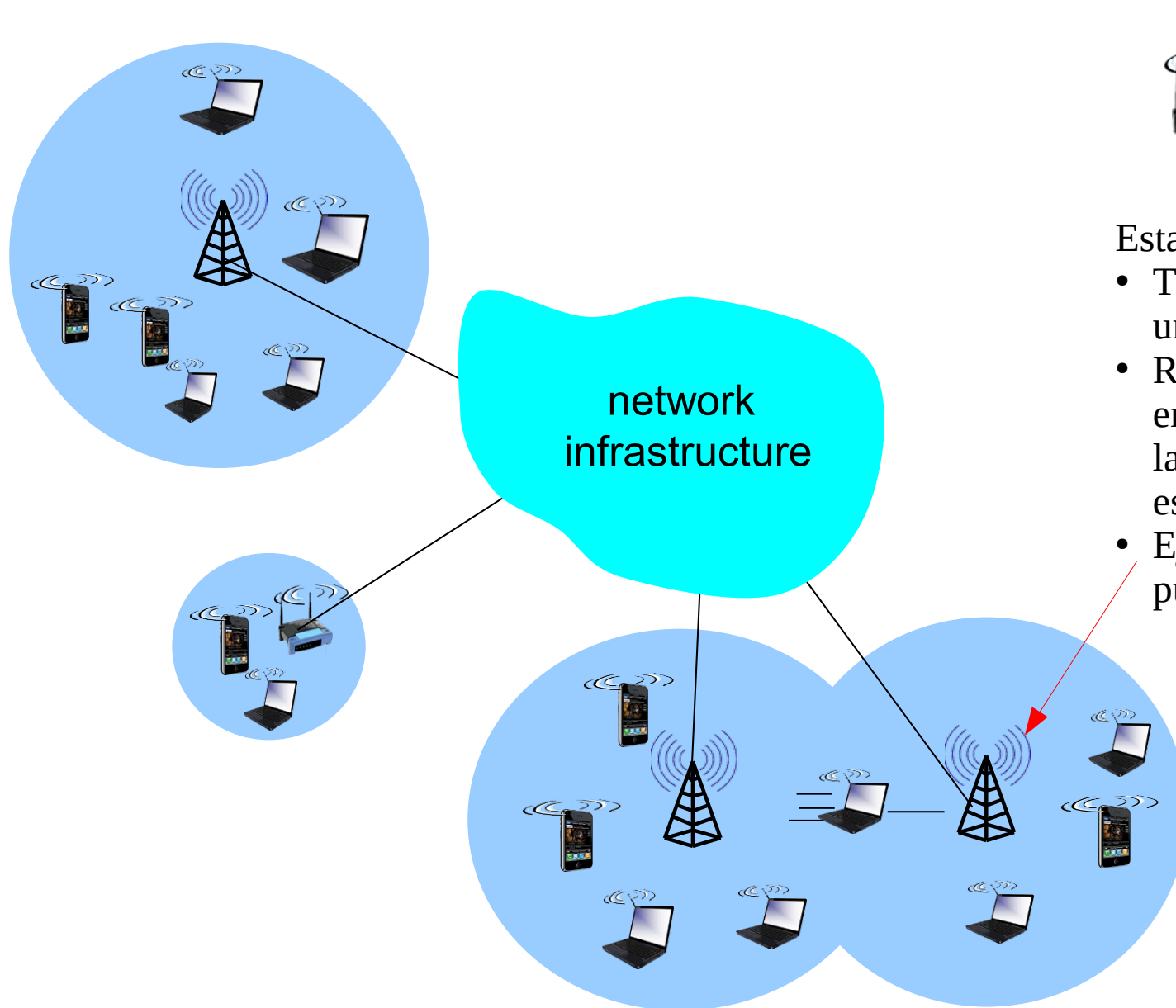
Elementos de una red inalámbrica



Elementos de una red inalámbrica



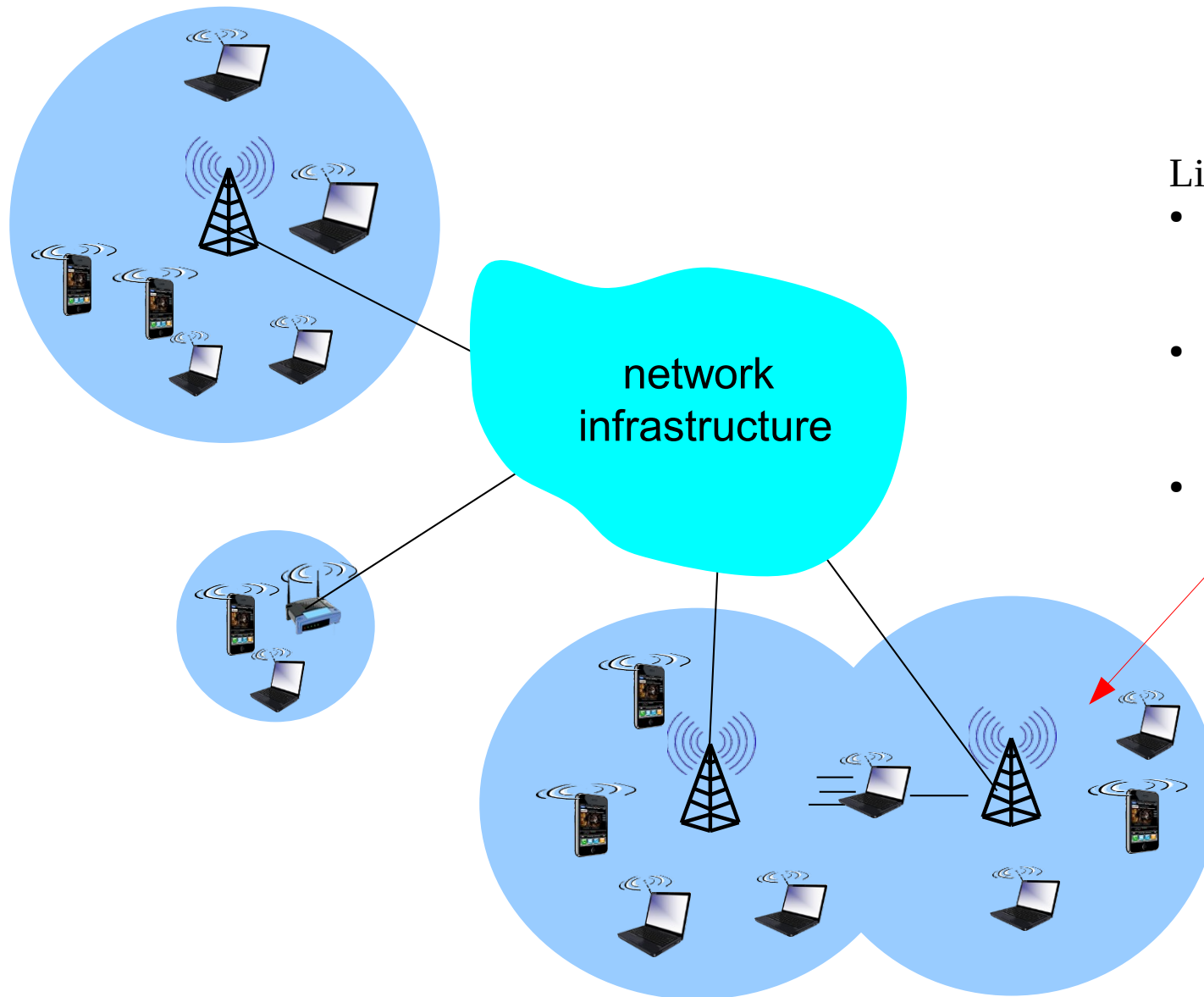
Elementos de una red inalámbrica



Estaciones Base

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

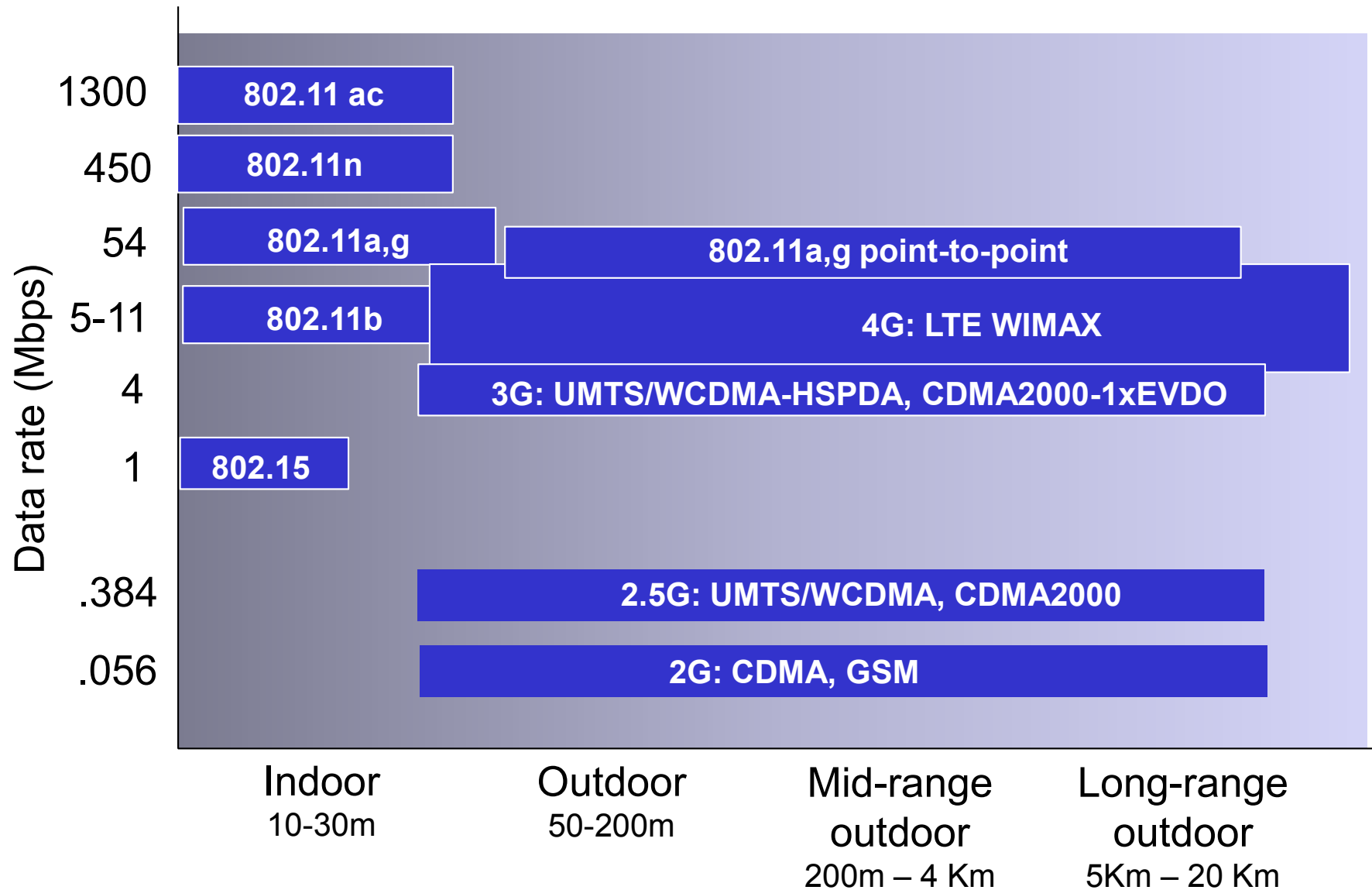
Elementos de una red inalámbrica



Links inalámbricos

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

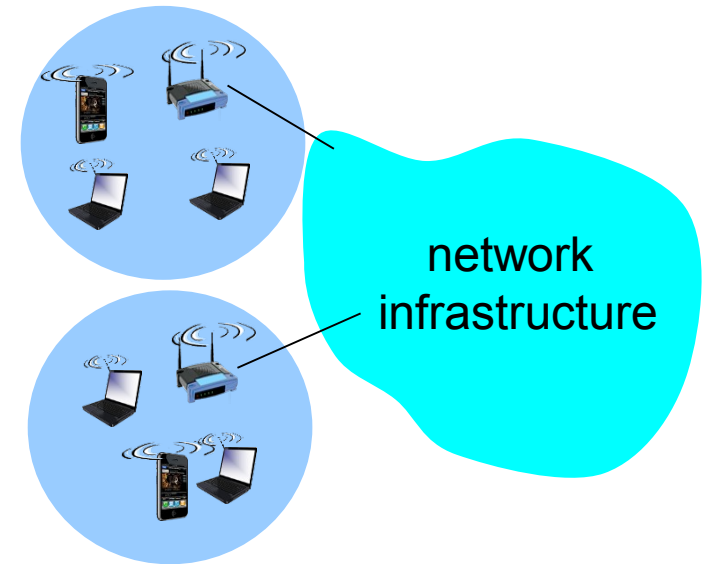
Ejemplos de algunas redes



Modo infraestructura vs. modo ad-hoc

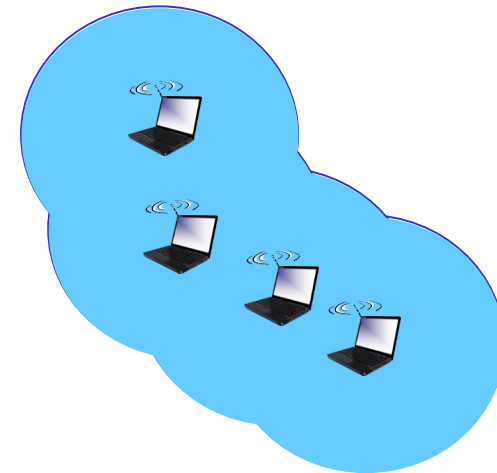
Modo infraestructura

- 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

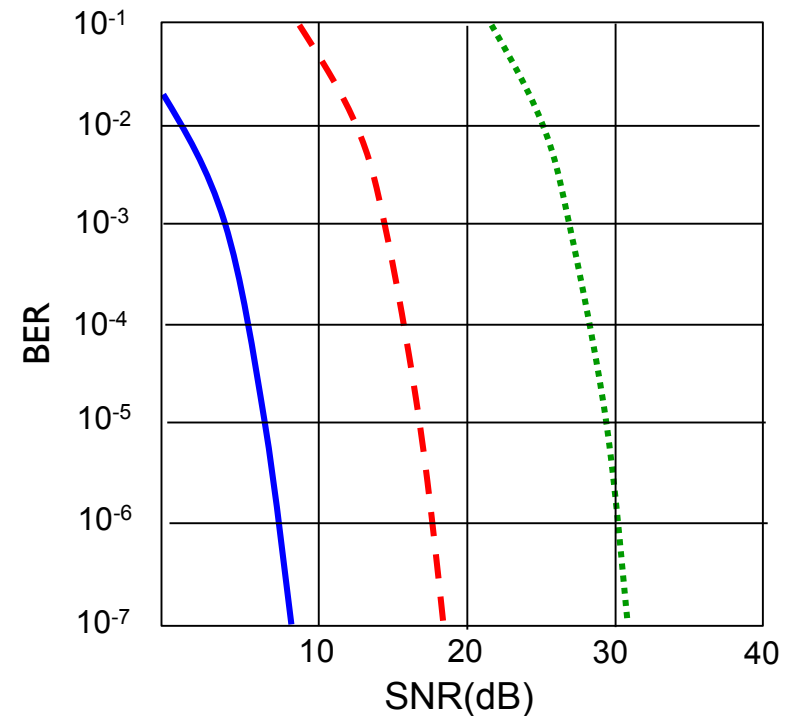


Características de los medios inalámbricos

- 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



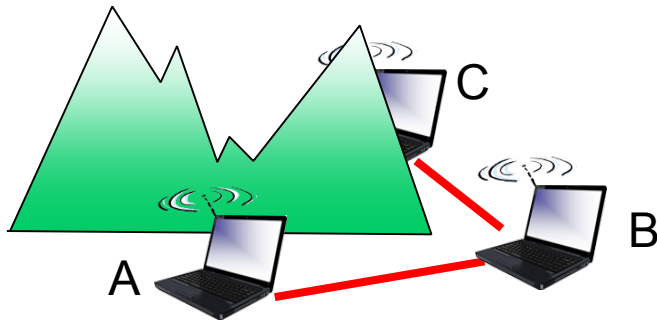
..... QAM256 (8 Mbps)

- - - QAM16 (4 Mbps)

— BPSK (1 Mbps)

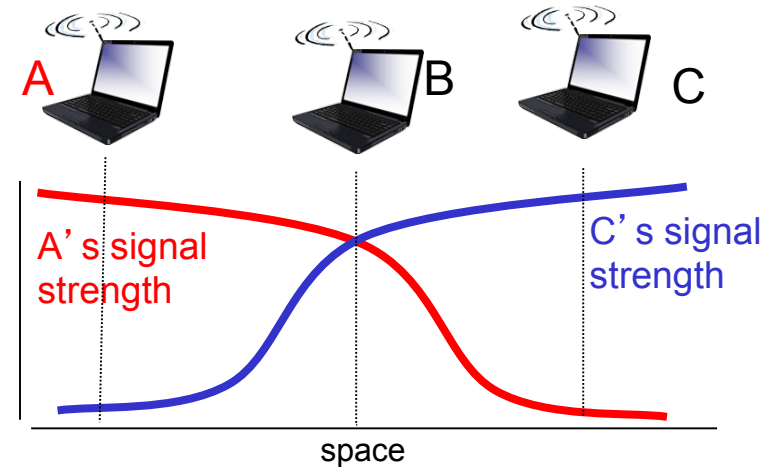
Interferencia en el receptor

- 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

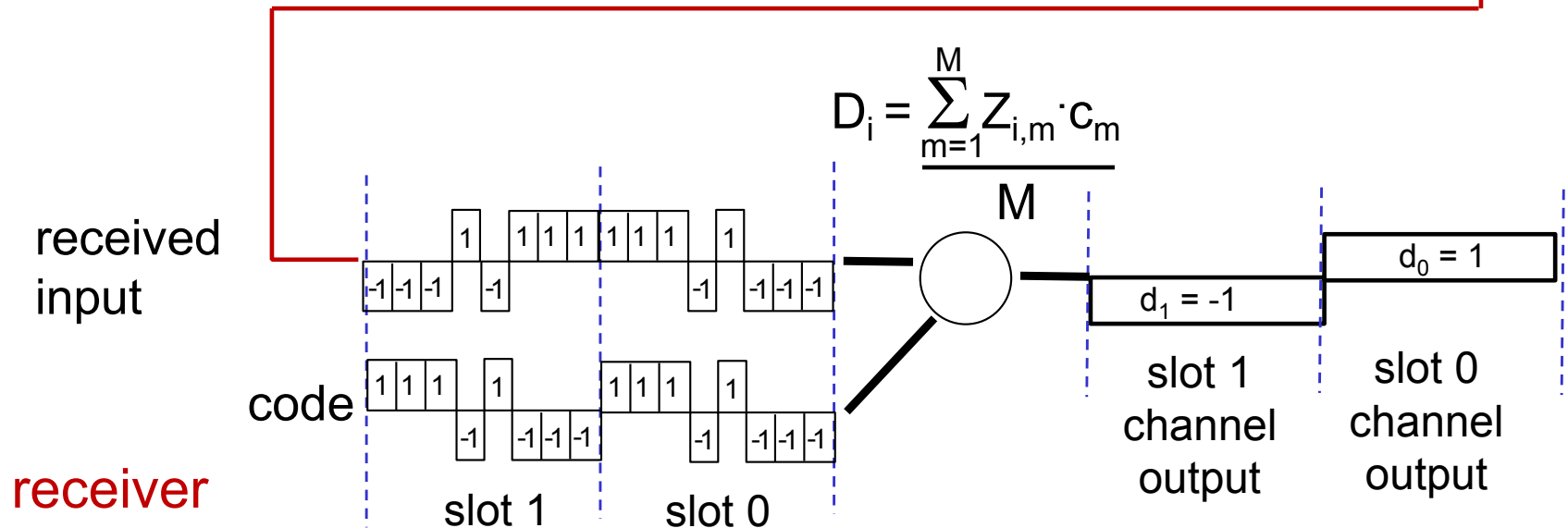
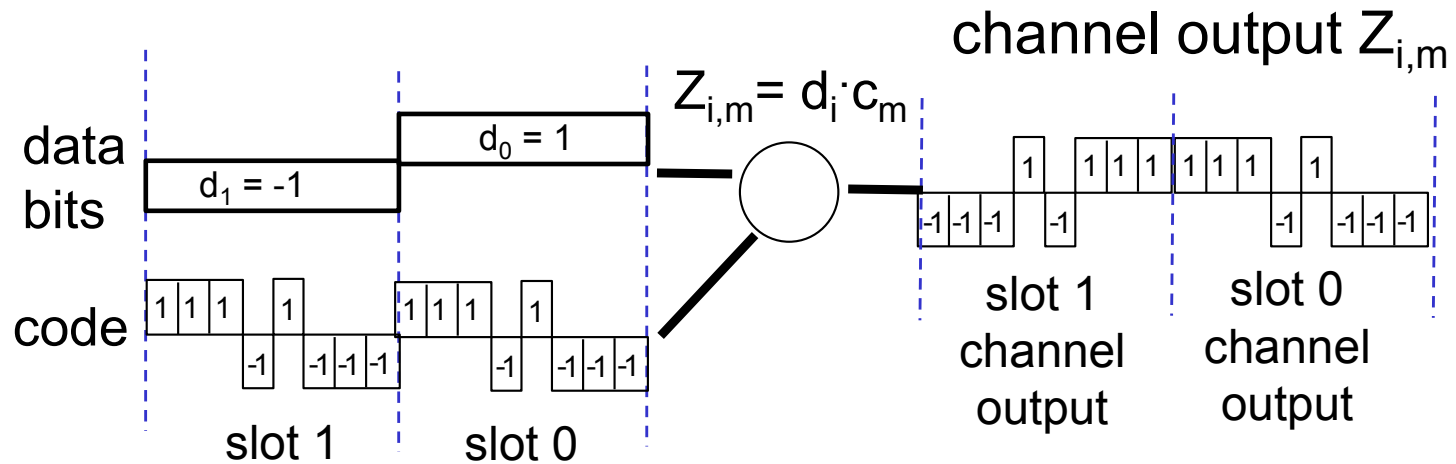
- B y A se escuchan
- B y C se escuchan
- A y C no se escuchan, no se dan cuenta que se interfieren en B

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) \times (chipping sequence)
- Decodificación: producto interno de la secuencia codificada con chipping sequence

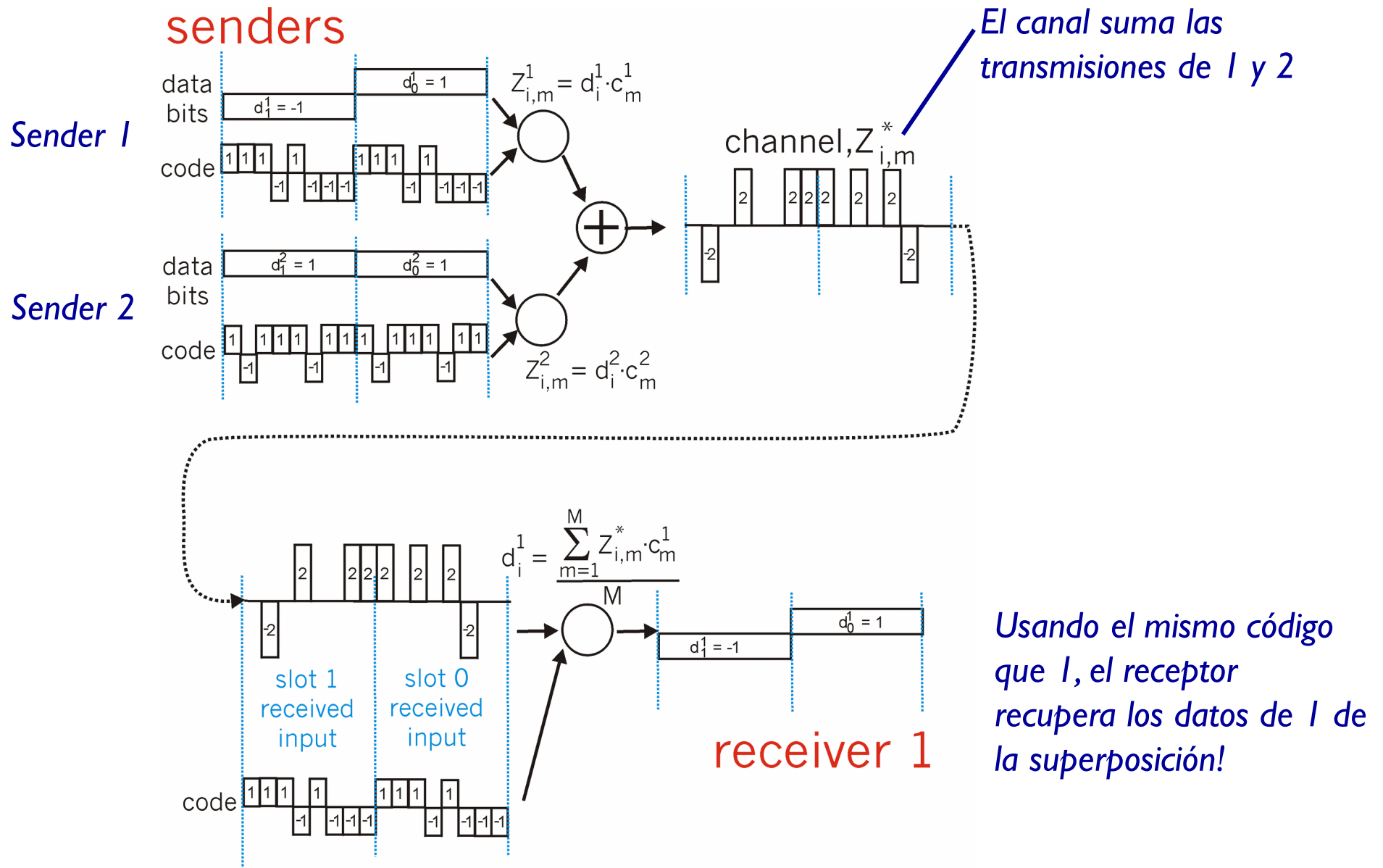
CDMA: Codificación/decodificación

sender



receiver

CDMA con múltiples transmisores



- 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)

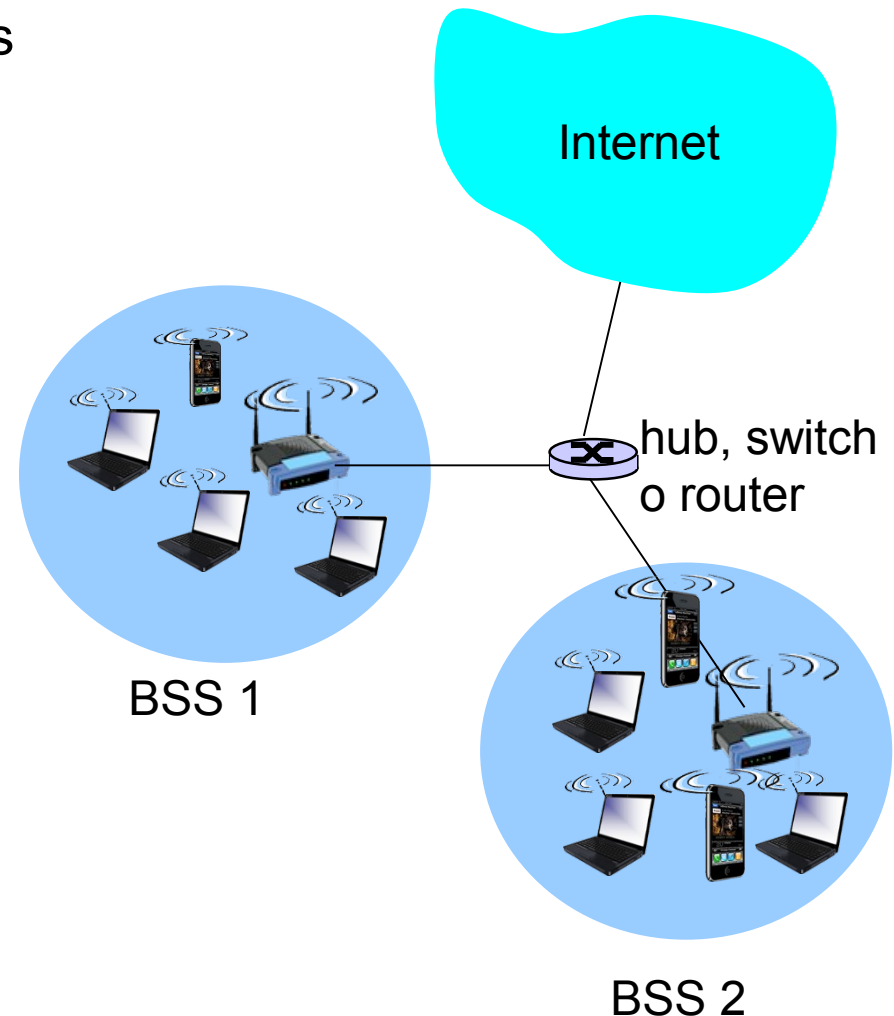
- Redes de área local inalámbricas
- Utilizan rangos de frecuencia reservados para uso sin licencia
 - 2.4 GHz (2400-2483 MHz)
 - 5,8 GHz (5725-5850 MHz)
- Deben ser resistentes a interferencia, ruido, etc
- Deben solucionar el acceso al medio compartido
- Deben solucionar el problema de las estaciones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

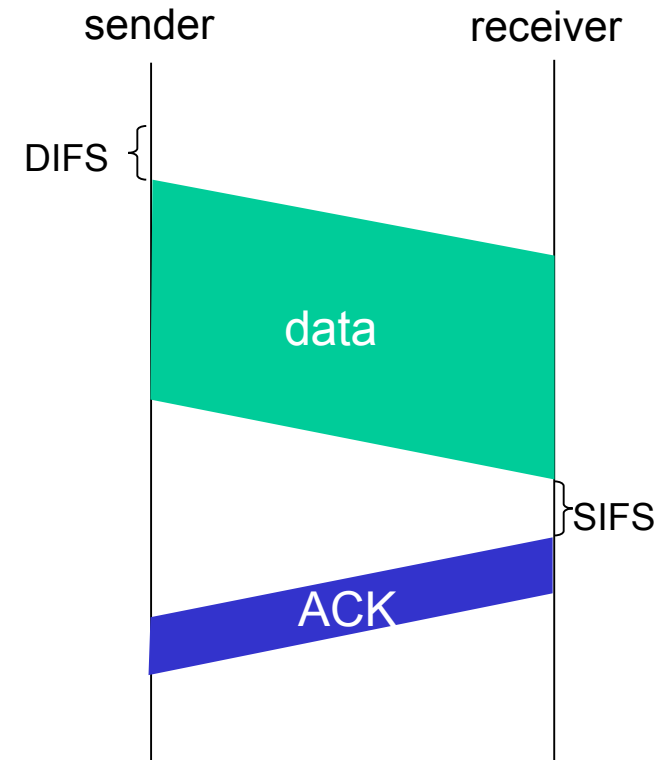
- Ej 802.11b: el espectro disponible (2,4 – 2,485 GHz) se divide en canales (11-12 dependiendo de la región)
- El canal a utilizar se configura administrativamente en el AP
 - Algunos APs pueden elegirlo automáticamente
- Interferencia posible con APs cercanos
- No todos los canales son disjuntos
- Los 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: sensor 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)

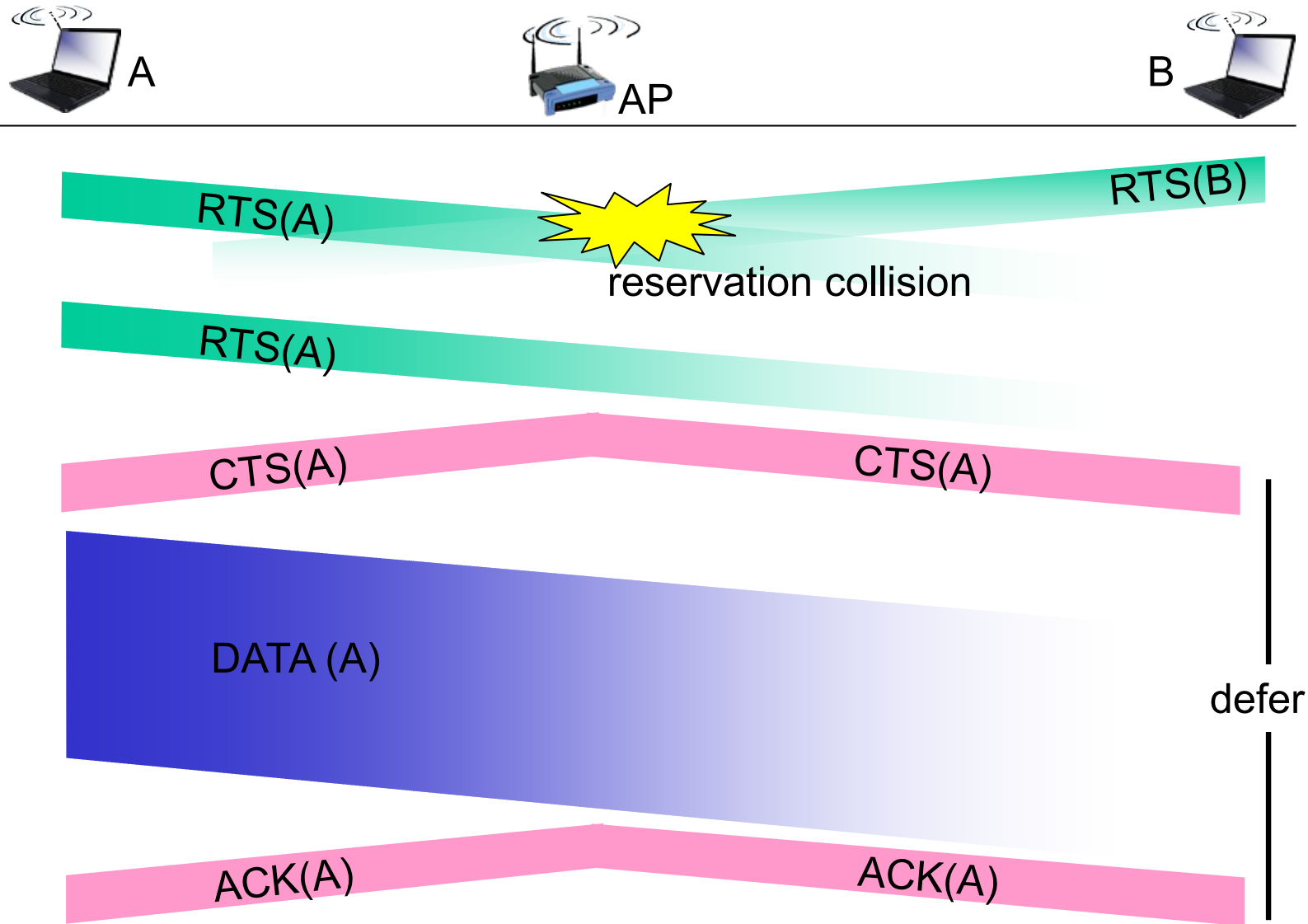
- Transmisor:
 - Si se observa el canal libre durante DIFS, entonces transmitir la trama
 - Si no se recibe ACK, debe retransmitirse
 - Si se observa el canal ocupado:
 - Random backoff time
 - Si el canal está libre, transmitir cuando vence el timer
 - Si no hay ACK, incrementar el tiempo de backoff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



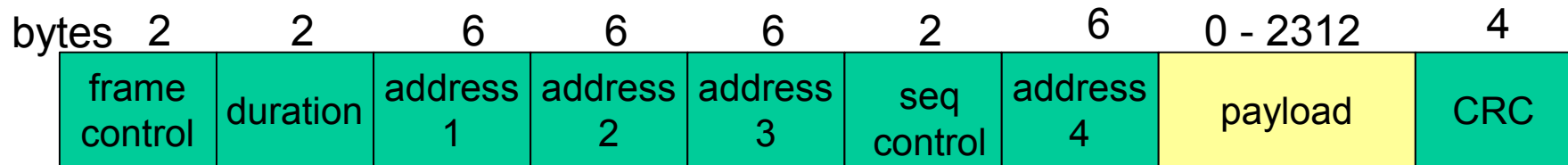
802.11 CSMA/CA (2)

- Para evitar colisiones (CA), queremos poder reservar el canal para evitar colisión de tramas largas
- Transmisor A envía trama corta de reserva (RTS) 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

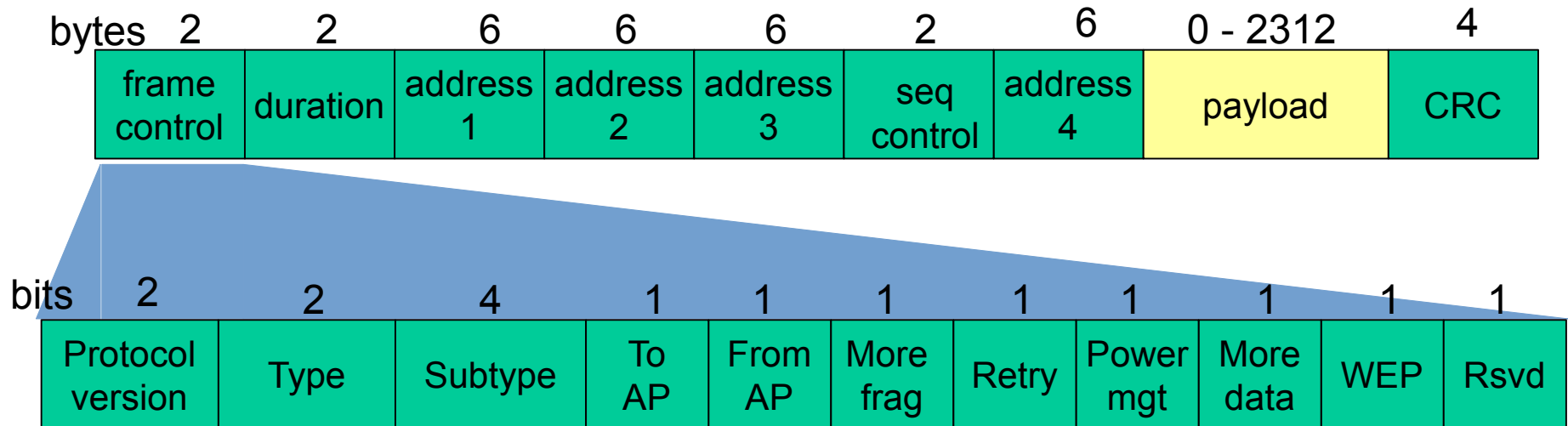


Trama 802.11



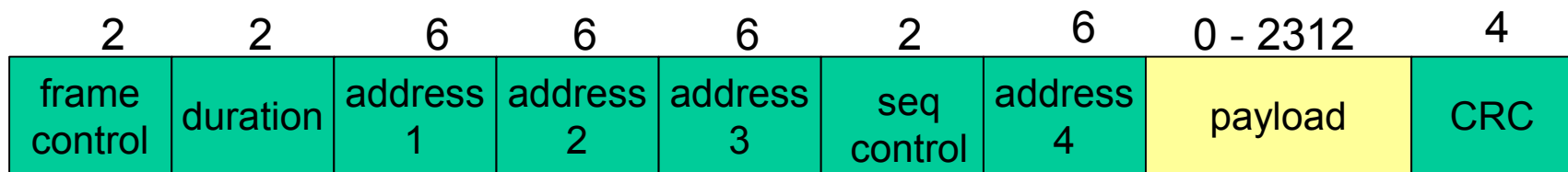
- Payload: carga útil de la trama
- CRC: detección de errores, 32 bits
- Duration: indicación de la duración de la reserva del canal (tanto en tramas de datos, como en RTS/CTS)
- Seq: número de secuencia (para tramas de datos). 12 bits (secuencia) + 4 bits (número de fragmento si fragmentamos)
 - Permite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

Trama 802.11: Frame Control



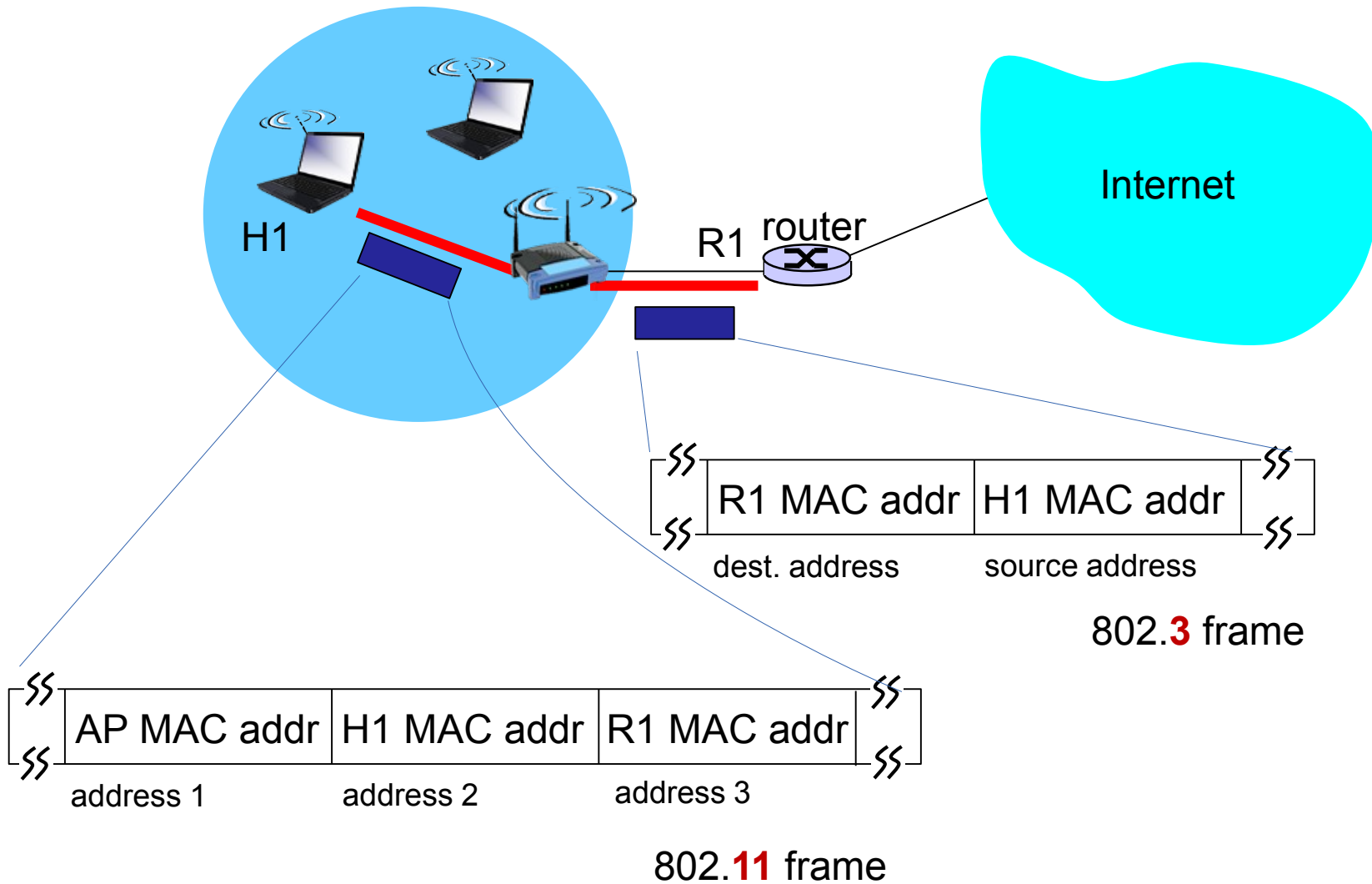
- Versión: 00
- Tipo y subtipo: datos, ACK, RTS, CTS, control, etc.
- To AP: trama destinada al AP
- From AP: trama con origen un AP
- More frag: hay más fragmentos de esta trama
- Retry: es una retransmisión
-

Trama 802.11: Direcciones



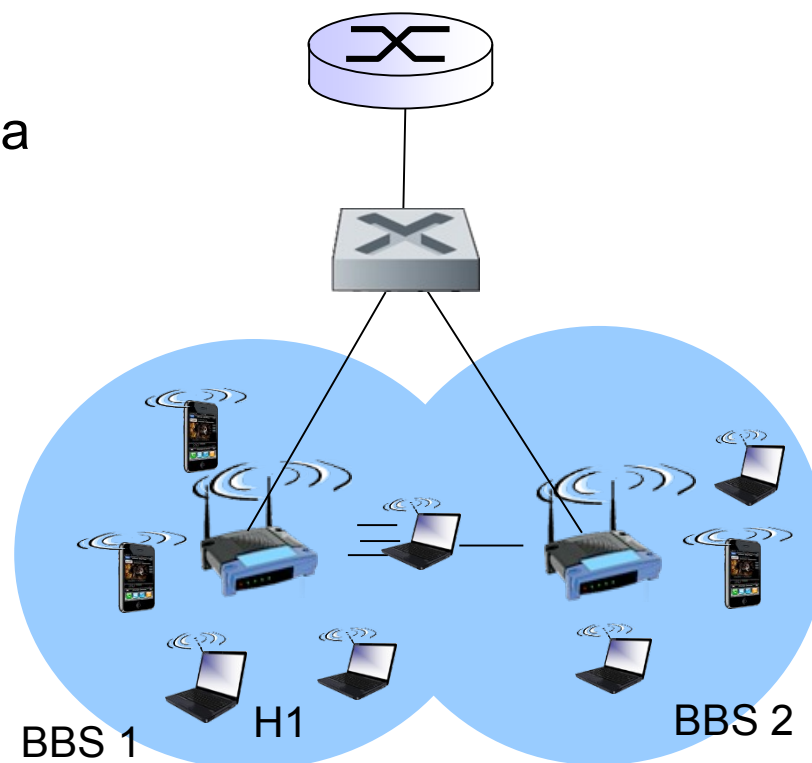
- Hasta 4 direcciones
- Address 1: destino (en el aire)
- Address 2: origen (en el aire)
- Address 3: dirección origen o destino finales
- Address 4: usada en links inalámbricos entre AP (redes mesh o WSS)

Ejemplo



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

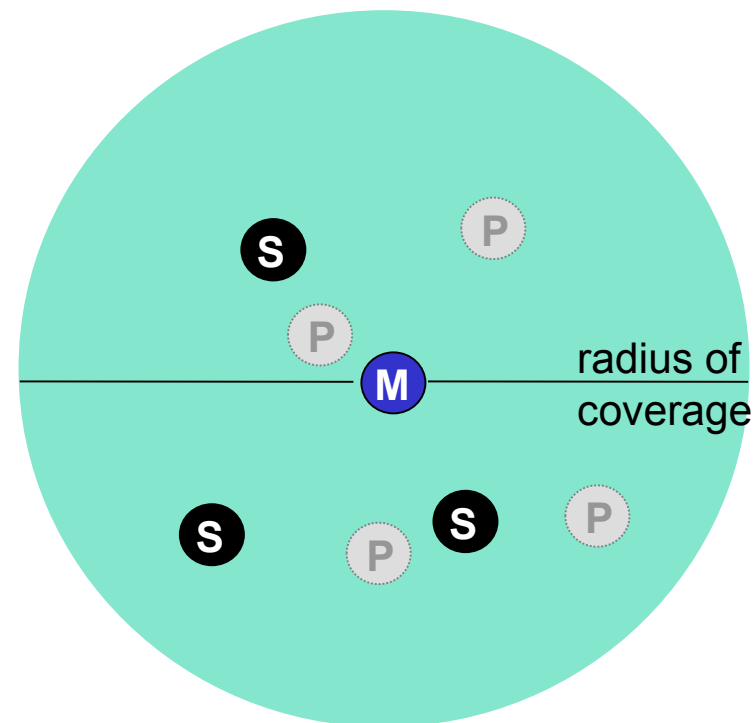


Modulación adaptativa, manejo de potencia

- ¿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 el AP 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



- M** Master device
- S** Slave device
- P** Parked device (inactive)