

Arquitectura de Redes, Sistemas y Servicios

Redes inalámbricas 802.11 y acceso al medio

Área de Ingeniería Telemática
Dpto. Automática y Computación
<http://www.tlm.unavarra.es/>

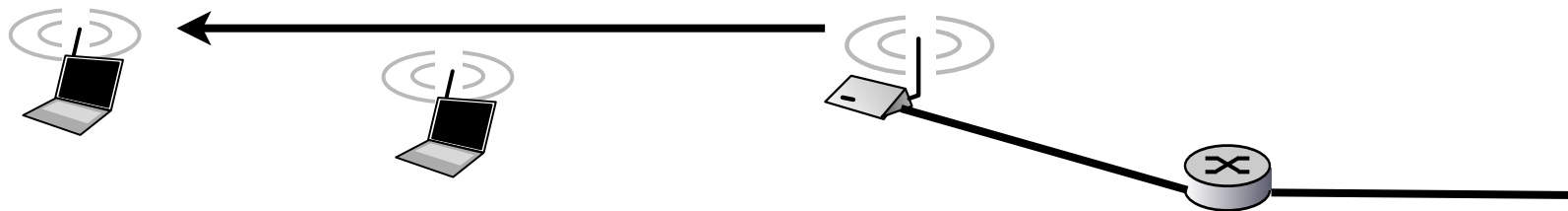
Redes inalámbricas

- ▶ Cada vez más importancia
ofrecen: movilidad, facilidad de instalación, flexibilidad
- ▶ Evolución hacia comunicaciones inalámbricas
Telefonia (GPRS,3G...), dispositivos WPAN (Bluetooth, wirelessUSB...) y **redes de datos** (802.11, WiMax?...)
- ▶ Nos centraremos en **IEEE 802.11** (vulgarmente wifi)

Wifi 802.11: Nivel físico

- ▶ NICs y puntos de acceso, transmiten y reciben señales de radio/microondas a través del aire
 - > Varios estándares de modulación
 - + DSSS, FHSS, Luz infrarroja en BB (no se utiliza)
 - > Y frecuencias
 - + 2.4GHz, 5GHz, 3GHz

Paquete modulado sobre portadora de 2.4GHz con DSSS
La velocidad de datos en el canal es 11Mbps



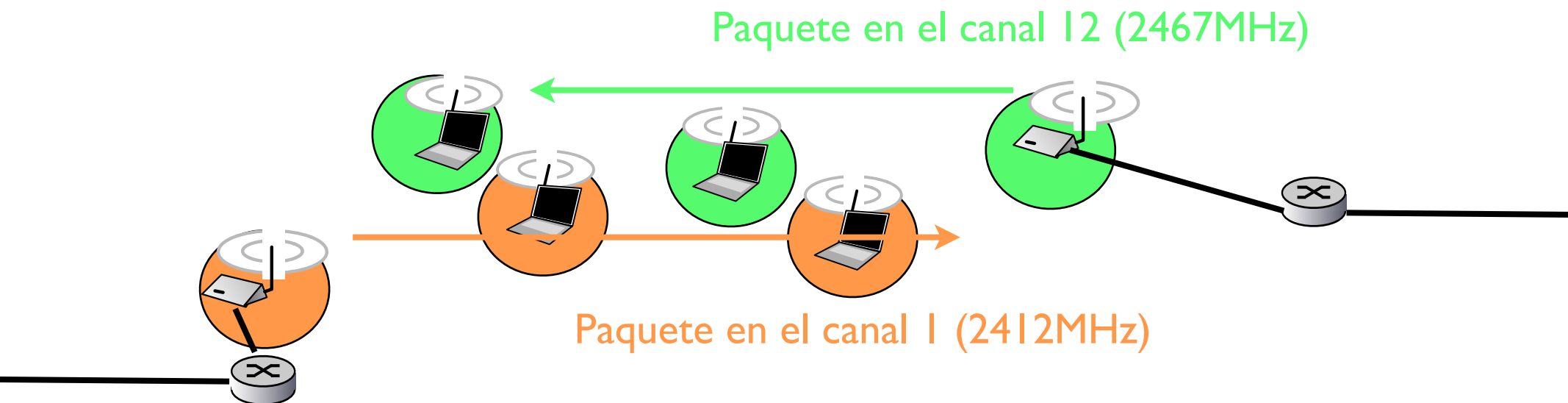
Medio compartido de broadcast

Las NICs oyen el paquete y según la cabecera lo procesan

Wifi 802.11: Nivel físico

- ▶ Versiones con el tiempo (definidos por diferentes estándares del IEEE)
- ▶ 802.11a 5GHz velocidad de datos hasta 54Mbps
- ▶ 802.11b 2.4GHz velocidad de datos hasta 11Mbps
- ▶ 802.11g 2.4GHz velocidad de datos hasta 54Mbps
- ▶ 802.11n 2.4,5GHz velocidad de datos hasta 248Mbps
- ▶ El espectro en torno a la frecuencia utilizada se divide en varios canales utilizando frecuencias cercanas.

Permite tener varias redes en el mismo espacio



Wifi 802.11: Nivel físico

- ▶ Canales en 802.11b

- > En la banda libre de 2.4GHz

- > Algunos son ilegales en algunos países

- EEUU 1-11

- EMEA 1-13

Canal	Frecuencia	Canal	Frecuencia
1	2412 MHz	8	2447 MHz
2	2417 MHz	9	2452 MHz
3	2422 MHz	10	2457 MHz
4	2427 MHz	11	2462 MHz
5	2432 MHz	12	2467 MHz
6	2437 MHz	13	2472 MHz
7	2442 MHz	14	2484 MHz

- ▶ Aún así los canales cercanos se interfieren

- ▶ De todas formas el mecanismo de acceso al medio es capaz de soportar varias redes en el mismo canal cercanas utilizando colisiones y CSMA

- ▶ Nos interesa más el nivel de enlace

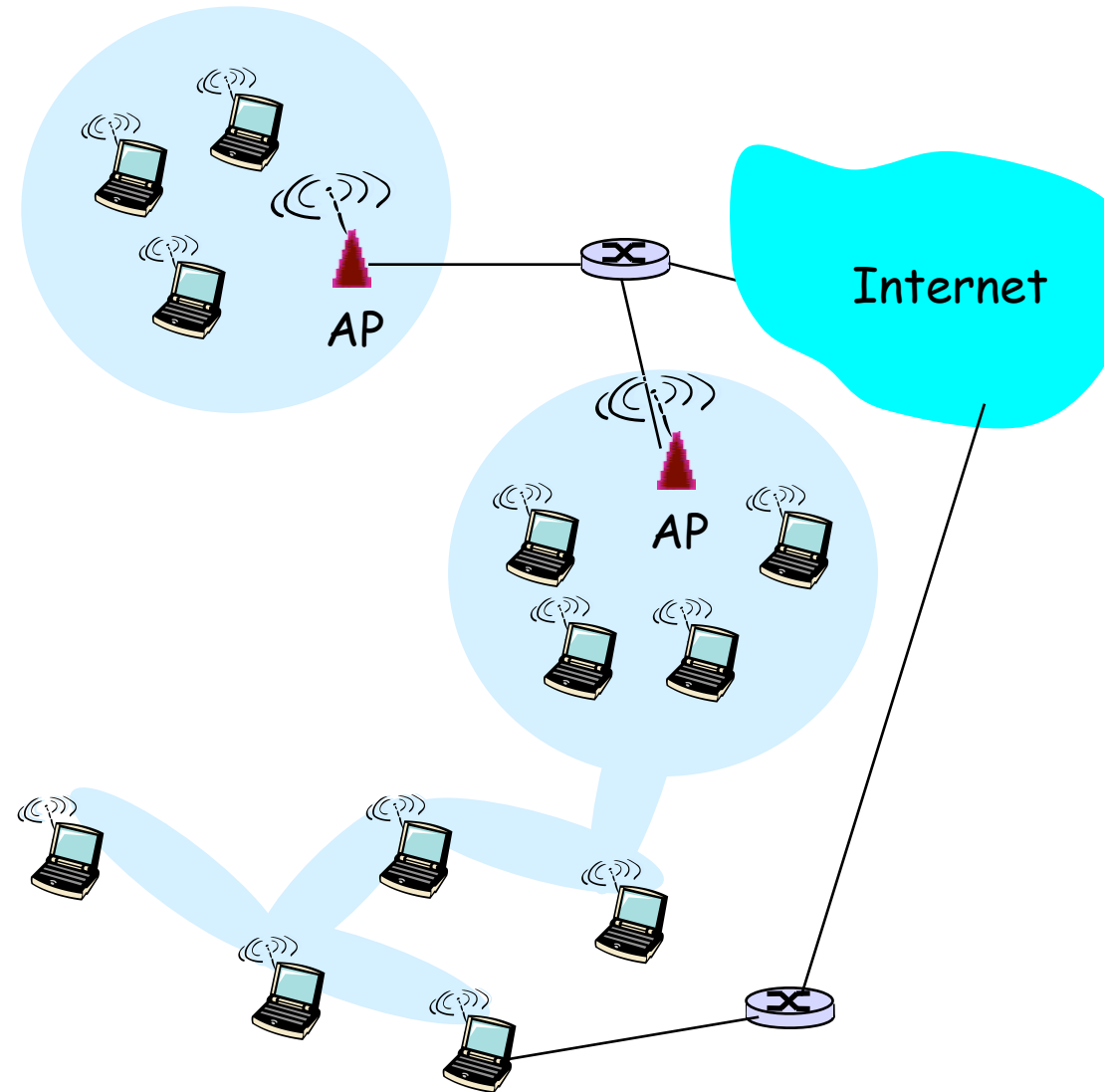
2 modos de funcionamiento

▶ **Base-station**

- > Infraestructura: estaciones base (access point) conectadas a una red fija

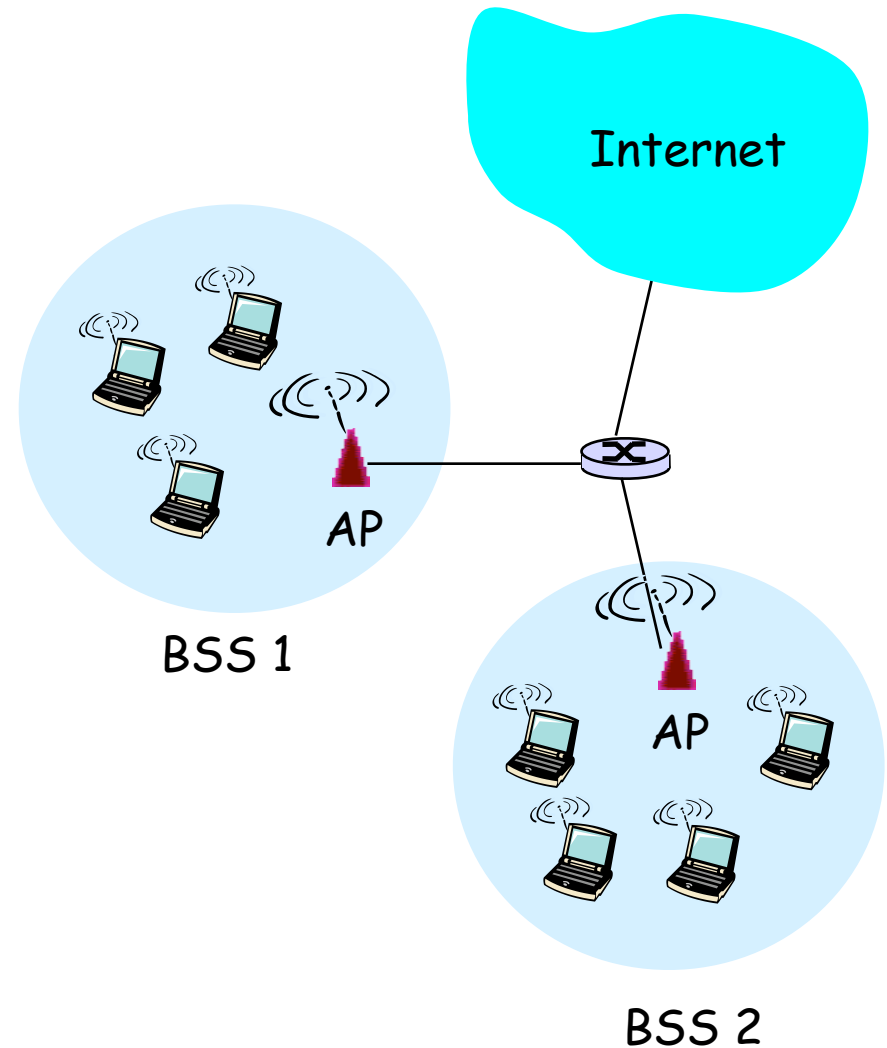
▶ **Ad-hoc**

- > punto-a-punto
- Los terminales inalámbricos se comunican entre si
- > Corren algoritmos de enrutamiento y extienden la red más allá del alcance de uno
- > parecido a peer-to-peer



Basic Service Set

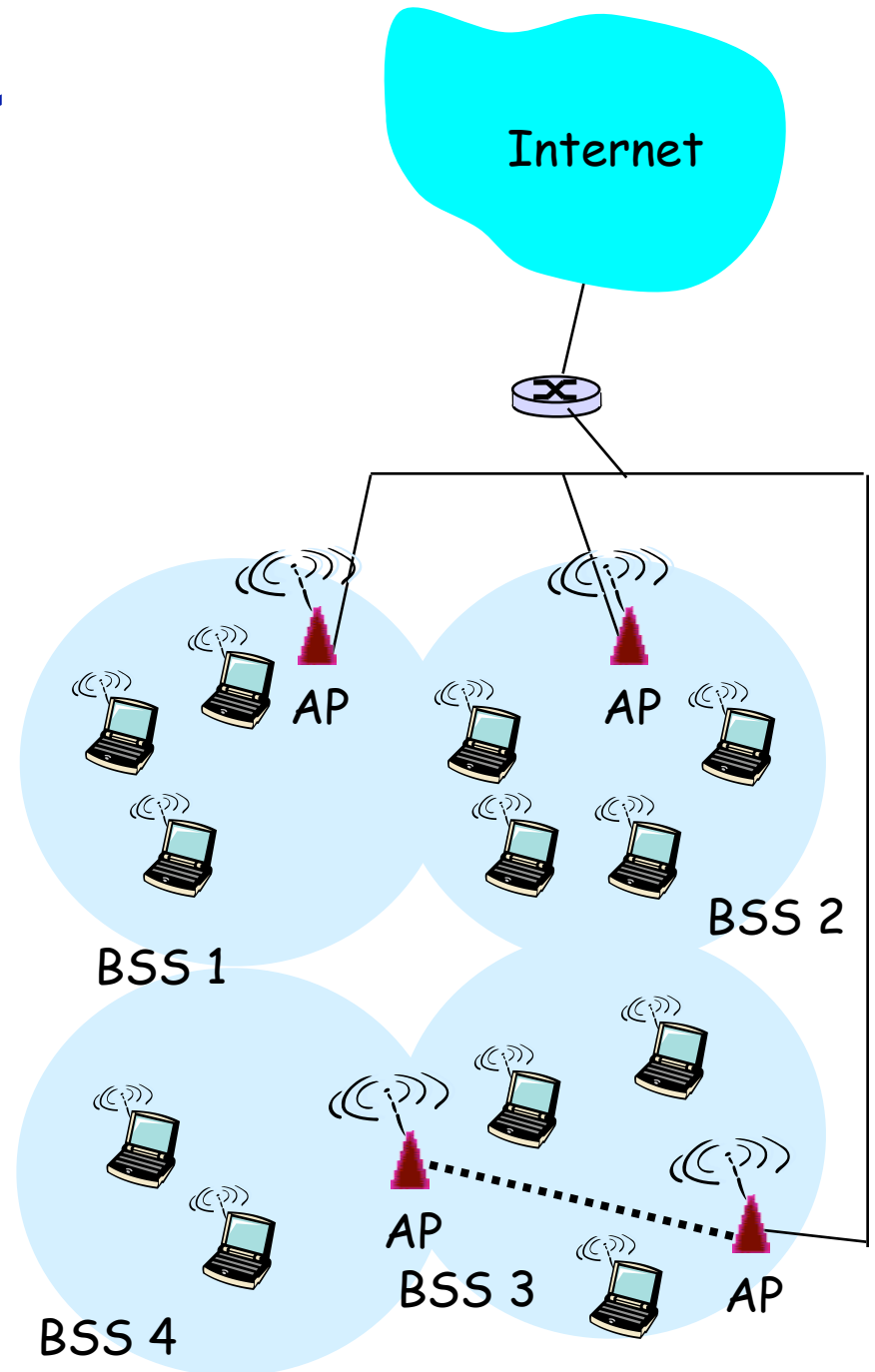
- ▶ Al conjunto formado por
 - > Hosts wireless
 - > 1 access point
 - > su router de acceso
- ▶ Le llamaremos Basic Service Set (BSS)
- ▶ Equivalentes a las celdas de la telefonía móvil



Extended Service Set

- ▶ Varios BSSs unidos para dar un servicio común en una zona mayor
- ▶ Le llamaremos Extended Service Set (ESS)
- ▶ La interconexión entre puntos de acceso puede ser por una red de cable o incluso wireless (WDS)
- ▶ El ESS tiene un identificador común de forma que el usuario no sabe si es un BSS o un ESS

El Service Set Identifier (SSID)



802.11 Asociación

- ▶ Para poder comunicarse en un BSS los hosts deben primero asociarse a la red deseada (identificada por su SSID)
- ▶ ¿Como conocen el SSID?
 - > La estación base envía periódicamente tramas (beacon) con su nombre (SSID) y su dirección MAC

Eso permite a los hosts escanear los canales y presentar al usuario los SSIDs observados para que elija

- > La estación base no envía tramas beacon (SSID oculto) y el administrador es responsable de configurar el SSID

Esto a veces se ve como una medida de seguridad pero es una medida de seguridad muy ligera. El SSID no se protege y si observas el canal y ves a otro host asociarse ves el SSID

802.11 Asociación

- ▶ Antes de transmitir un host sigue los pasos:
 - > Escanea permanentemente los canales en busca de tramas beacon (y los presenta al usuario para que elija o está configurado para buscar unos SSIDs que conoce)
 - > Una vez elegido el SSID realiza autenticación y asociación
 - + Pide autorización al Access Point para estar en la red
 - Varios protocolos que permiten comprobar si el usuario tiene acceso a la red (con contraseña (SKA), autenticación abierta (OSA) que siempre se concede)
 - + Pide al Access Point que lo considere asociado a la red
 - Al completar este protocolo el host está en el BSS
 - > Una vez realizada el host forma parte del BSS y puede enviar tramas (de nivel de enlace 802.11) a otros hosts del BSS o al router. El access point reenvía las tramas que recibe de ese host al medio
 - Normalmente lo primero que hace el host es usar protocolos de configuración de IP, enviar petición de DHCP para obtener IP y parámetros de configuración IP en la red de la estación

802.11 Asociación

existe una red llamada

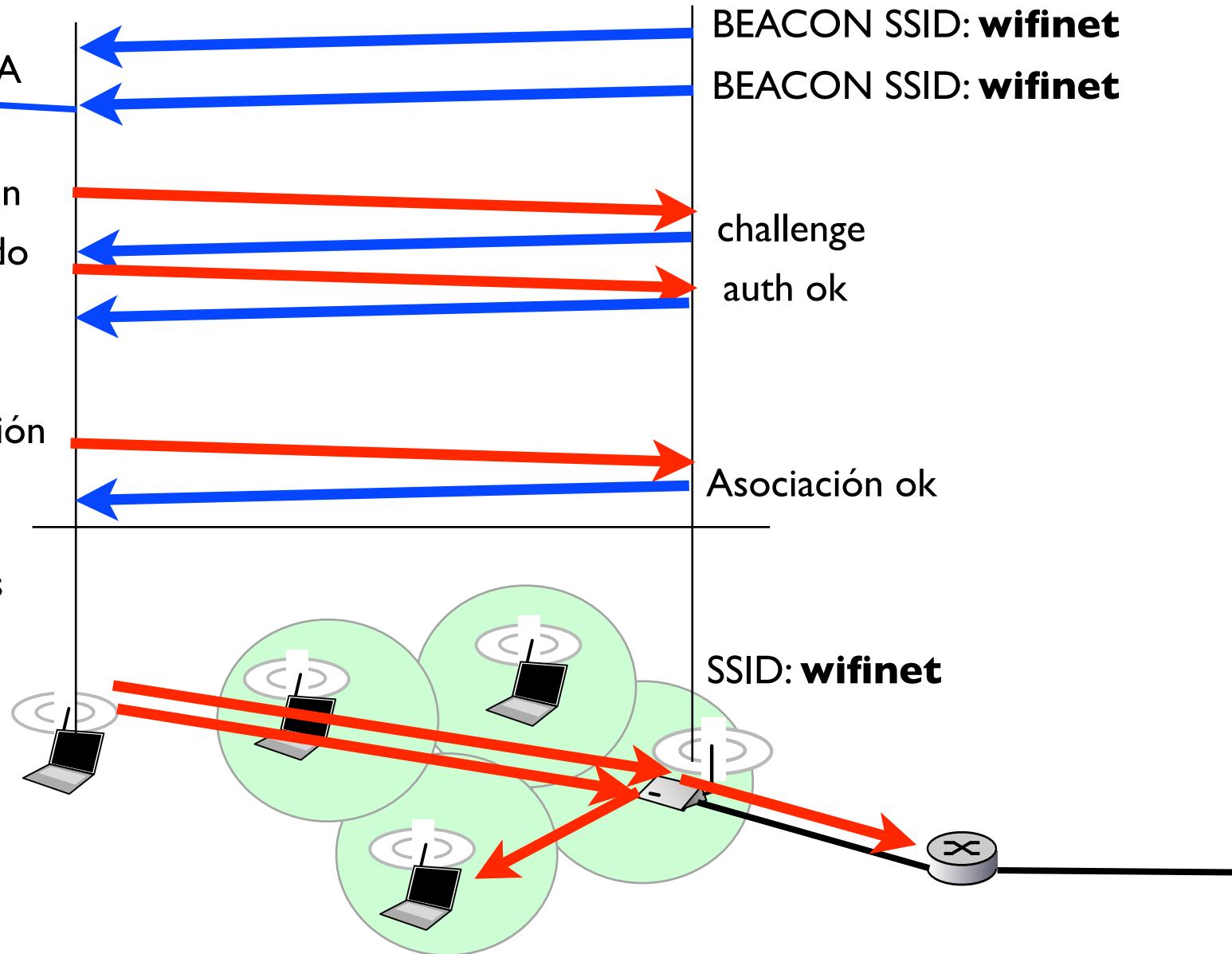
wifinet

y usa autenticación SKA
(shared key auth)

Peticion autenticación
challenge cifrado

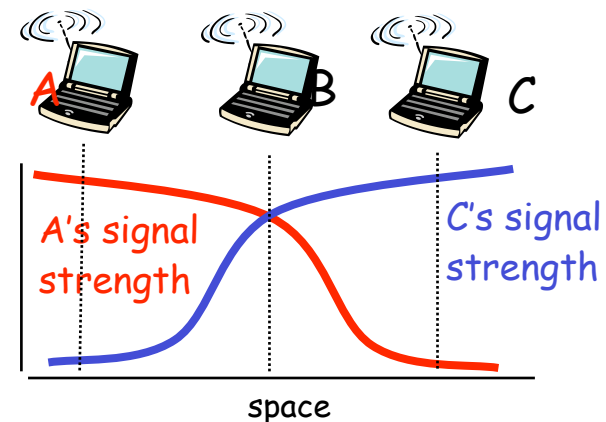
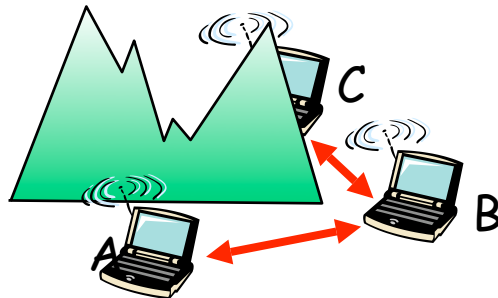
Peticion asociación

A partir de aqui puedo
enviar a los demas hosts
y al router



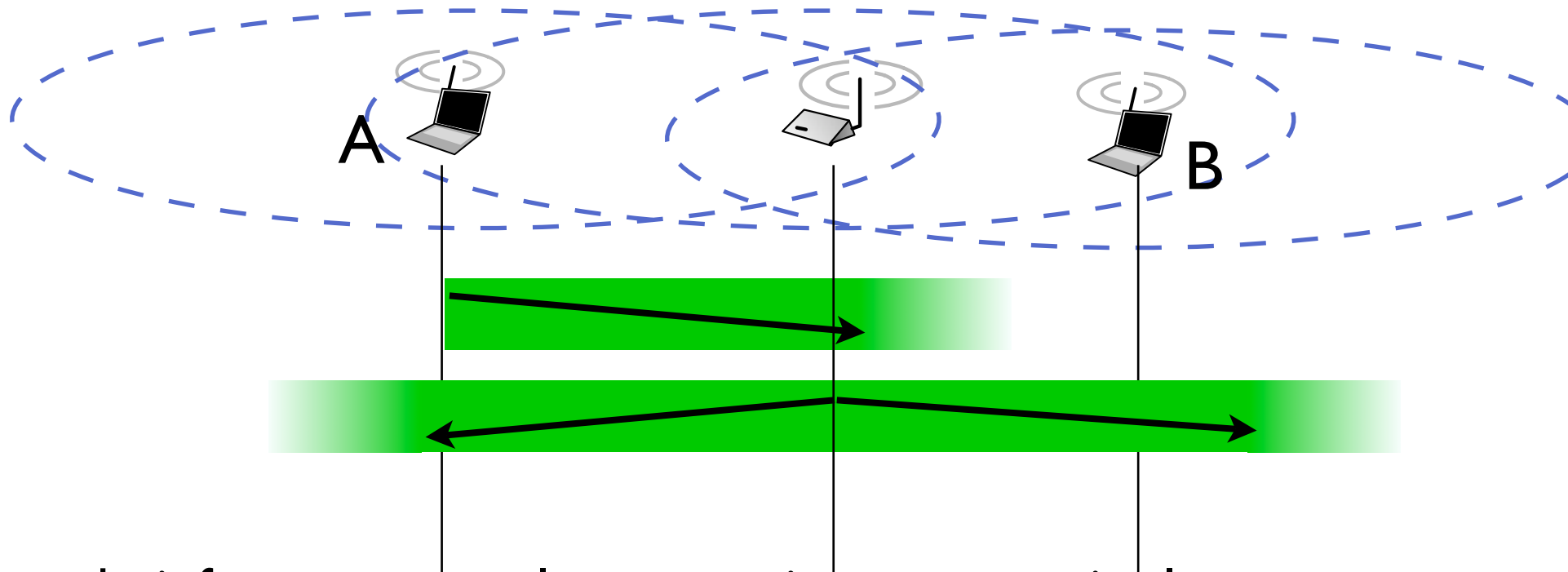
802.11 Acceso múltiple

- ▶ Acceso múltiple con problemas propios del medio inalámbrico
- ▶ Usa CSMA (carrier sense, si veo que alguien está enviando no envío)
 - > No colisiona con transmisiones en curso
- ▶ Pero la detección de colisión es un problema
 - > La señal se atenúa muy rápido por lo que es difícil comparar lo enviado con lo recibido. De hecho normalmente las NIC no pueden escuchar mientras envían
 - > Existe el problema de terminales ocultos
 - A y C no se oyen entre si
 - No pueden saber que B ve una colisión



802.11 Acceso múltiple

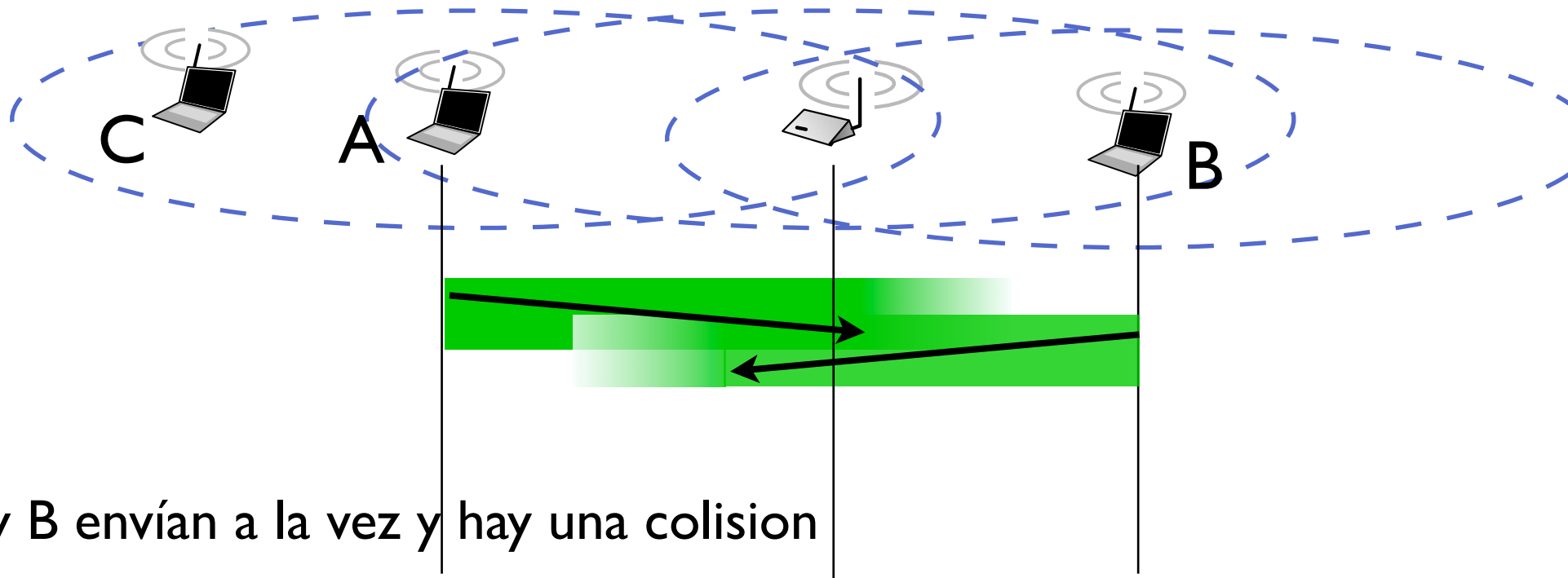
- ▶ Problemas de potencia:
 - > A oye al Access Point pero no a B



- ▶ En modo infraestructura el access point retransmite las tramas para que las oigan todos los hosts del BSS
Las transmisiones host-host pasan siempre por el access point
- ▶ **Esto no soluciona el problema del terminal oculto**

802.11 Acceso múltiple

- ▶ Si A y B quieren enviar a la vez a C ...



- ▶ A y B envían a la vez y hay una colisión

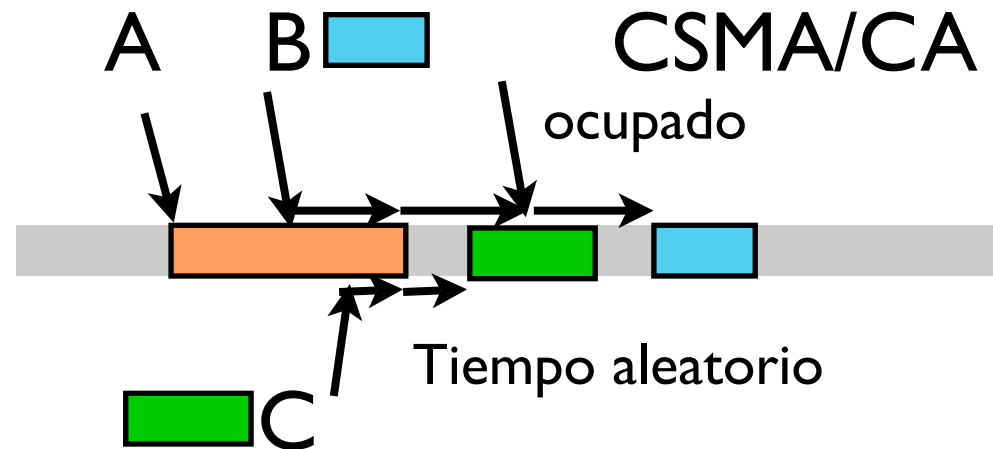
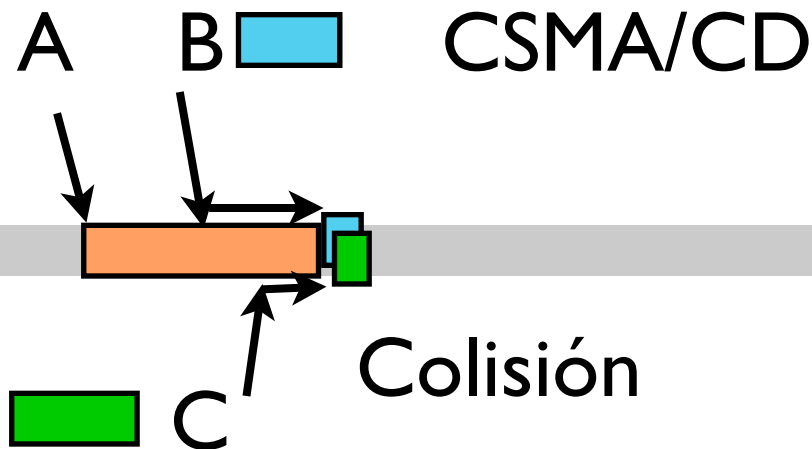
El access point no recibe ninguno

Pero ni A ni B pueden detectar la colisión porque están lejos

- ▶ El access point no reenvía ninguno de los dos así que a C no recibe nada

CSMA/CA

- ▶ Collision avoidance (evitación) en lugar de detección
- ▶ El receptor confirma (ACK) las tramas (ante los problemas para detectar si ha habido colisión)
- ▶ Se utilizan tiempos aleatorios cuando voy a transmitir
 - > Las colisiones son caras porque no se pueden detectar rápido. 1-persistente es demasiado agresivo y provoca colisiones
 - > Objetivo: evitar las colisiones causadas entre las estaciones que esperan que el medio quede libre
 - > No persistente



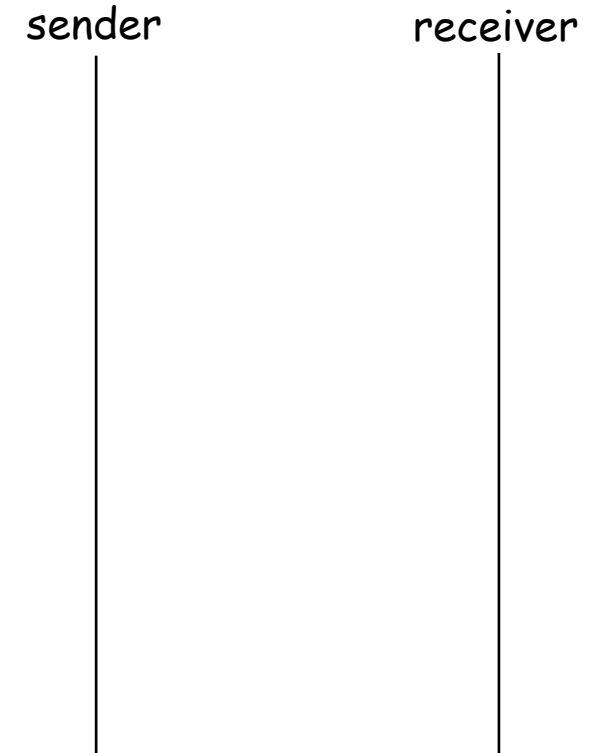
CSMA/CA

▶ Emisor 802.11

- > Si el canal está vacío por un tiempo DIFS
 - + Envía la trama entera (sin CD)
- > Si el canal está ocupado
 - + Inicia un temporizador aleatorio (con backoff)
 - + El temporizador solo descuenta tiempo con canal libre
 - + Transmite cuando expire
 - + Si no recibe ACK aumenta el backoff

▶ Receptor 802.11

- > Si recibo una trama
 - + Envía ACK después de un SIFS
($SIFS < DIFS$ los ACKs tienen prioridad)



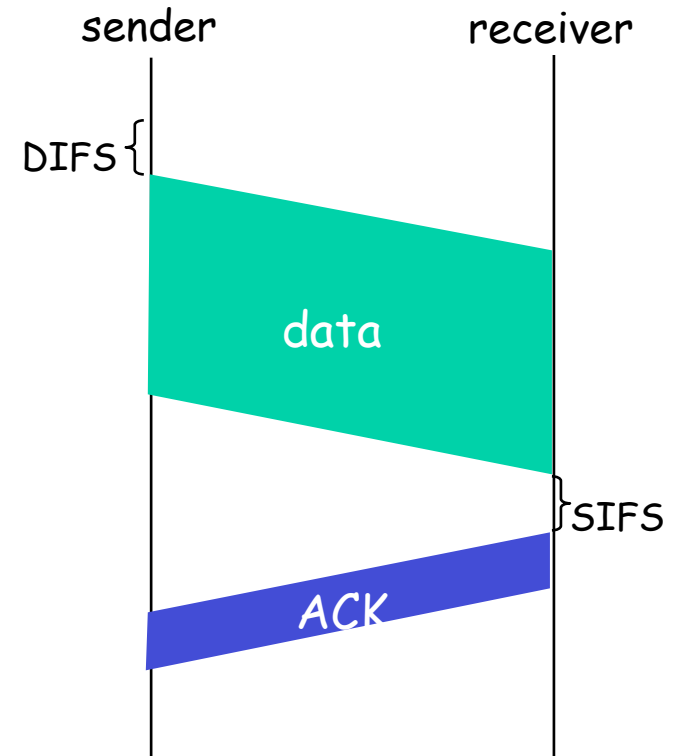
CSMA/CA

▶ Emisor 802.11

- > Si el canal está vacío por un tiempo DIFS
 - + Envía la trama entera (sin CD)
- > Si el canal está ocupado
 - + Inicia un temporizador aleatorio (con backoff)
 - + El temporizador solo descuenta tiempo con canal libre
 - + Transmite cuando expire
 - + Si no recibe ACK aumenta el backoff

▶ Receptor 802.11

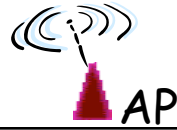
- > Si recibo una trama
 - + Envía ACK después de un SIFS
($SIFS < DIFS$ los ACKs tienen prioridad)



CSMA/CA

- ▶ Mejora: permitir al emisor reservar el canal para evitar colisiones en las tramas muy largas
 - > El emisor envía una trama de RTS (request to send) a la estación base pidiendo el canal (usando CSMA/CA)
Los RTS pueden colisionar con otras tramas pero al menos son cortas
 - > La estación base envía el permiso en una trama CTS (Clear to send)
 - > Todos los nodos reciben la CTS
 - + El solicitante envía la trama
 - + El resto dejan libre el canal
- ▶ Evita completamente las colisiones
 - > A costa de más retardo
 - > Normalmente se activa sólo para tramas por encima de una longitud

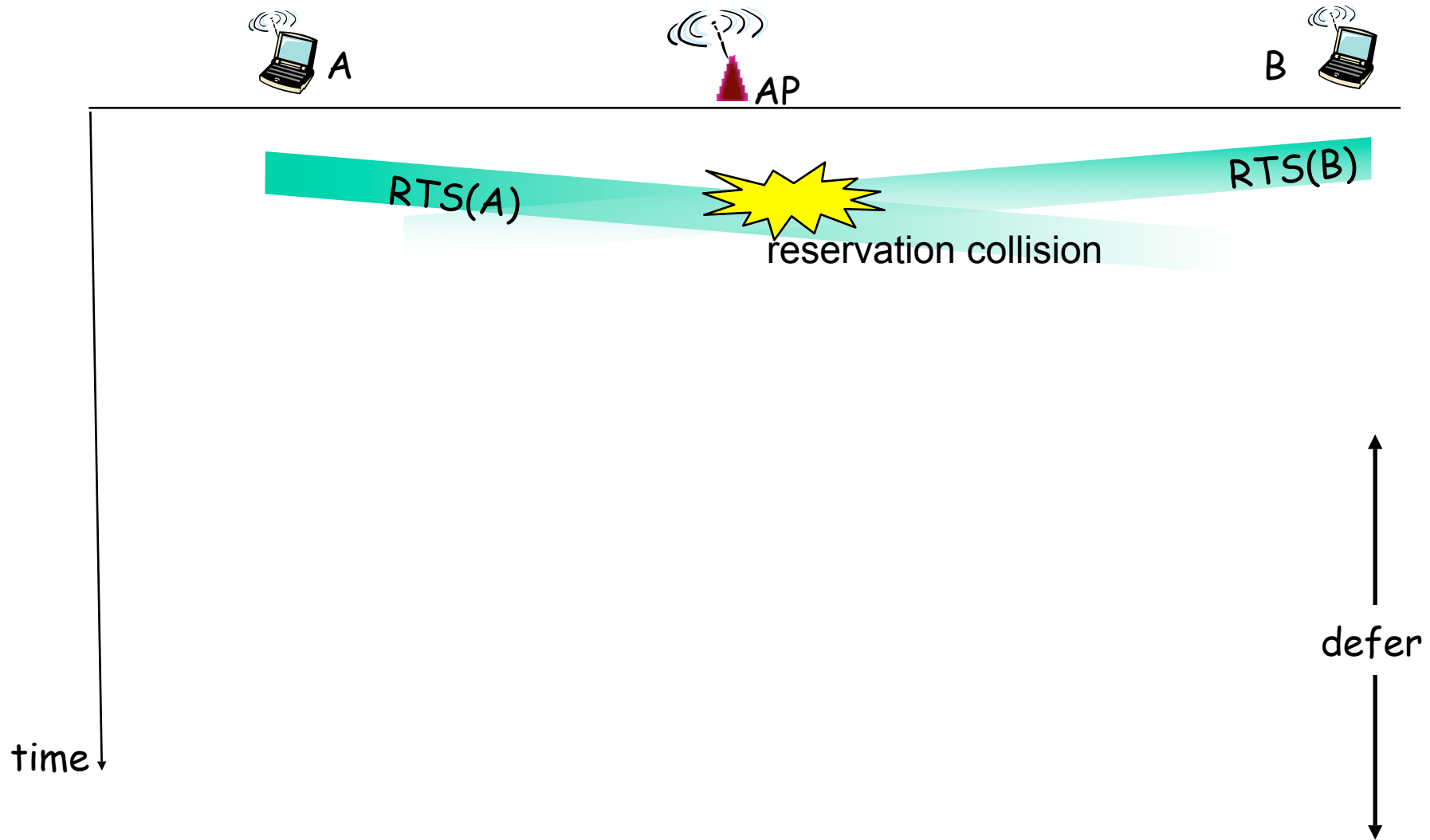
Ejemplo



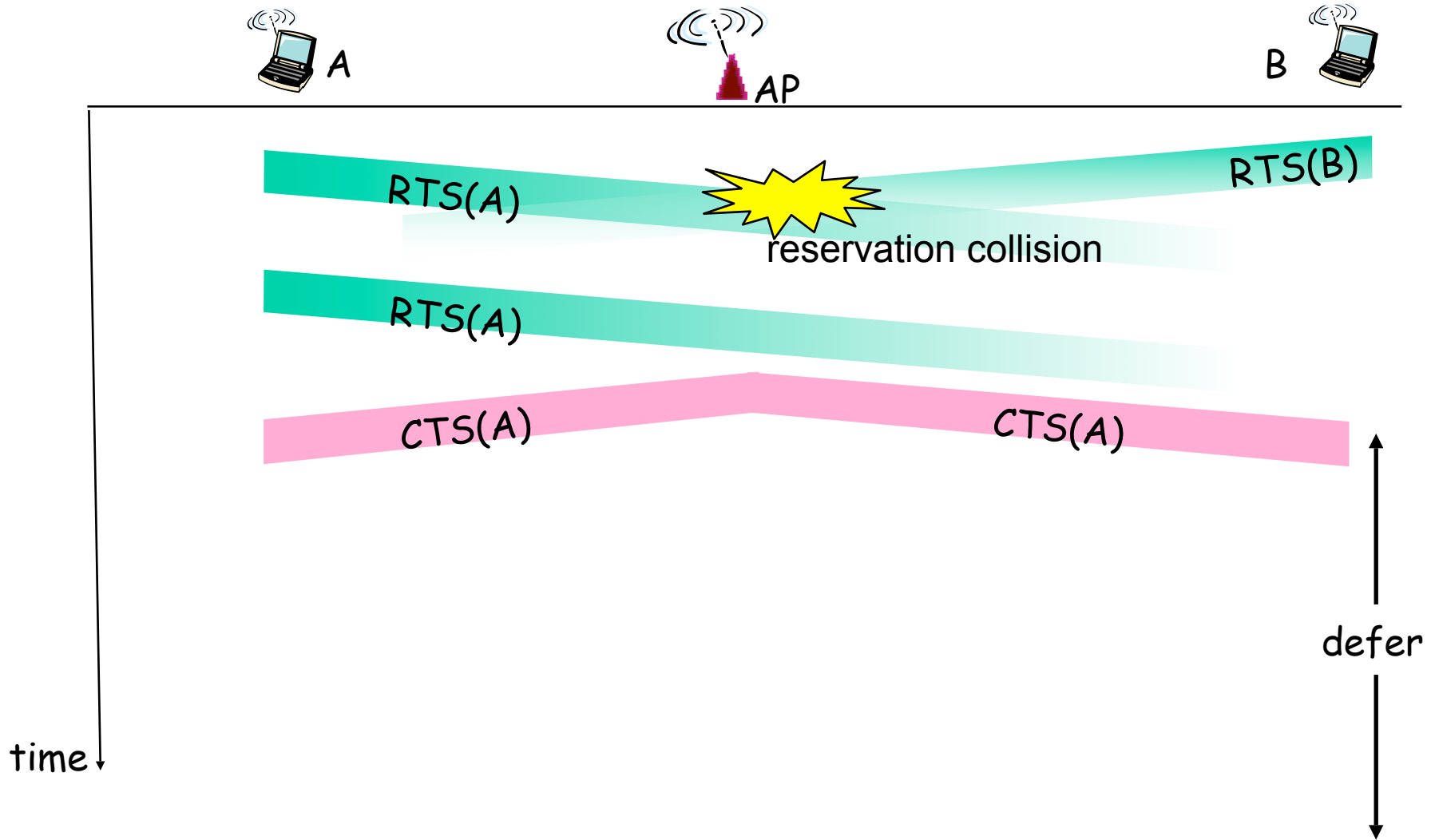
time ↓

↑
defer
↓

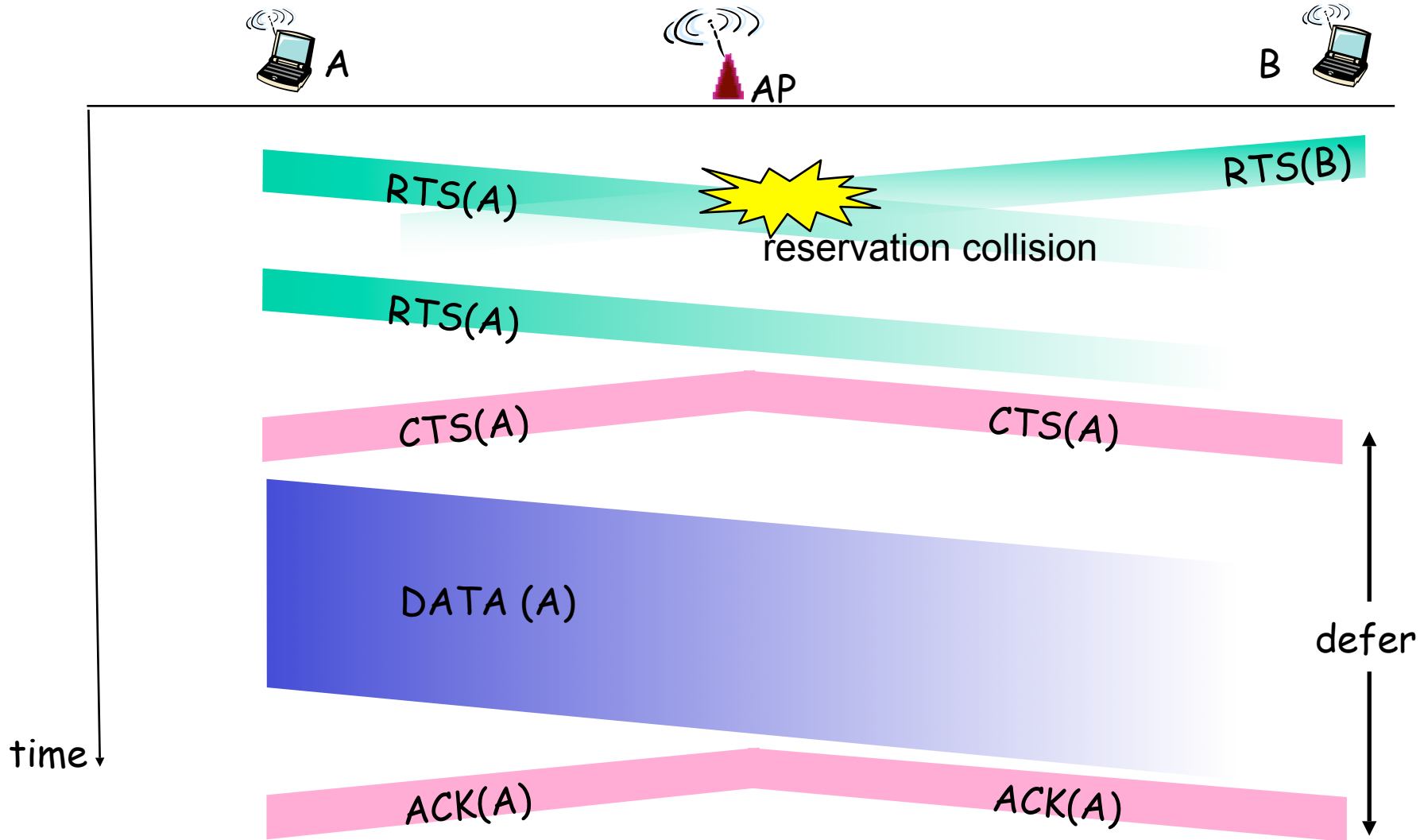
Ejemplo



Ejemplo



Ejemplo



Coordination function

- ▶ Esto es conocido como funcionamiento con función de coordinación distribuida

DCF

- ▶ El estándar también soporta tipo polling

Point Coordination Function (PCF)

- ▶ En modo Adhoc solo se usa la DCF
- ▶ En modo infraestructura se puede usar DCF o DCF+PCF
 - > Contention Free Periods (con PCF) + Contention Periods (con DCF)
- ▶ Pero PCF no se usa mucho
- ▶ 802.11e HCF Hybrid Coordination Function y soporte de QoS

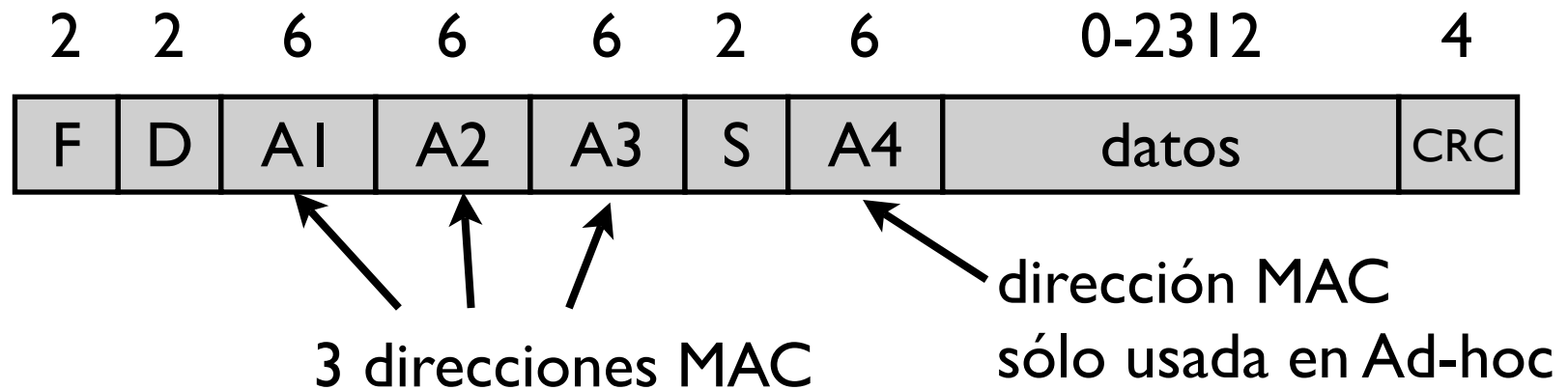
Resumiendo

- ▶ Control de acceso al medio más complicado que en Ethernet
 - > Hay ACKs en el nivel de enlace
 - > Hay retransmisiones en el nivel de enlace
 - > Hay autentificación/asociación
 - > El access point retransmite tramas
 - > CSMA
 - > Pero CSMA/CA en lugar de CD, colisiones costosas mejor evitar
 - > Se pueden usar técnicas de reserva de canal

Extras

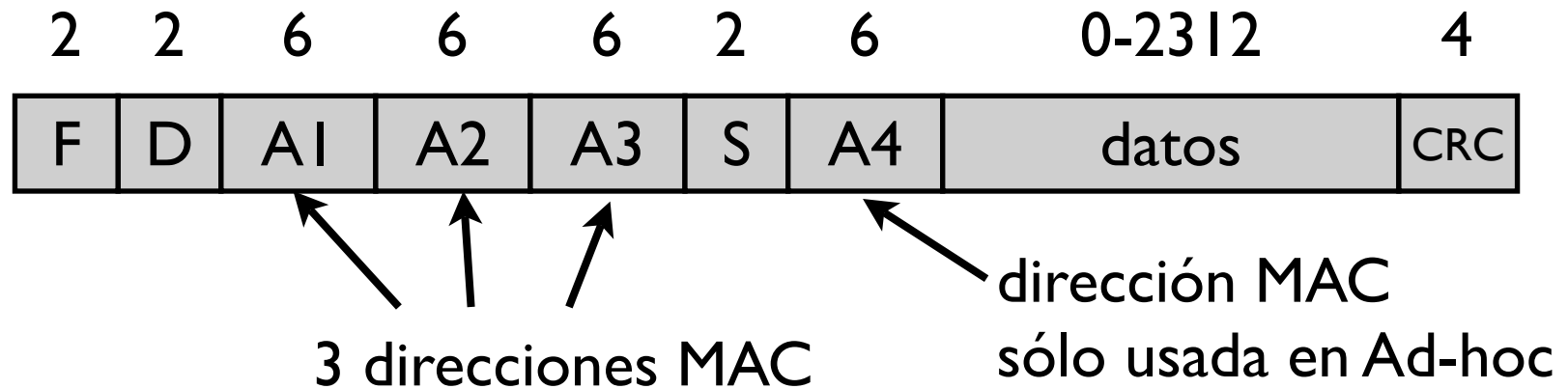
- ▶ Formato de tramas de 802.11
- ▶ Seguridad en 802.11

802.11: formato de trama



- ▶ S: secuencia de la trama
 - > necesario para el ACK
- ▶ 4 direcciones MAC
 - > A1: MAC destino. Wireless host que debe recibir esta trama
 - > A2: MAC origen. Wireless host que envia esta trama
 - > A3: MAC router asociado al access point
 - > A4: usada en modo Ad-hoc o para interconectar access-points a traves de la red inalambrica (WDS)

802.11: formato de trama



- ▶ F frame control
 - > Flags y tipo de la trama (Data, ACK, RTS o CTS)
- ▶ D duración
 - > Tiempo por el que se solicita el canal
En RTS/CTS

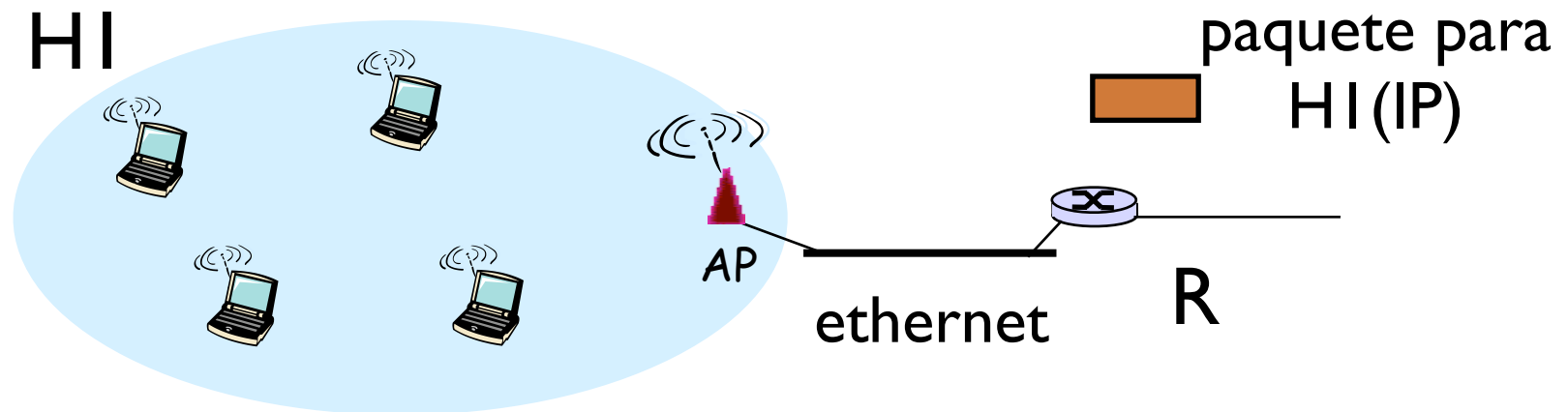
802.11 tipos de tramas

- ▶ El campo de control de la trama permite definir tipos y subtipos de tramas

Tipo	Subtipo	Nombre
00 (Management)	0	Asociación (request)
	1	Asociación (response)
	100	Probe request
	101	Probe response
	1000	Beacon
	otros
01 (Control)	1011	RTS
	1100	CTS
	1101	ACK
	...	otros
10 (Datos)	0	Datos
	otros opciones y QoS
11 (No se usa)		

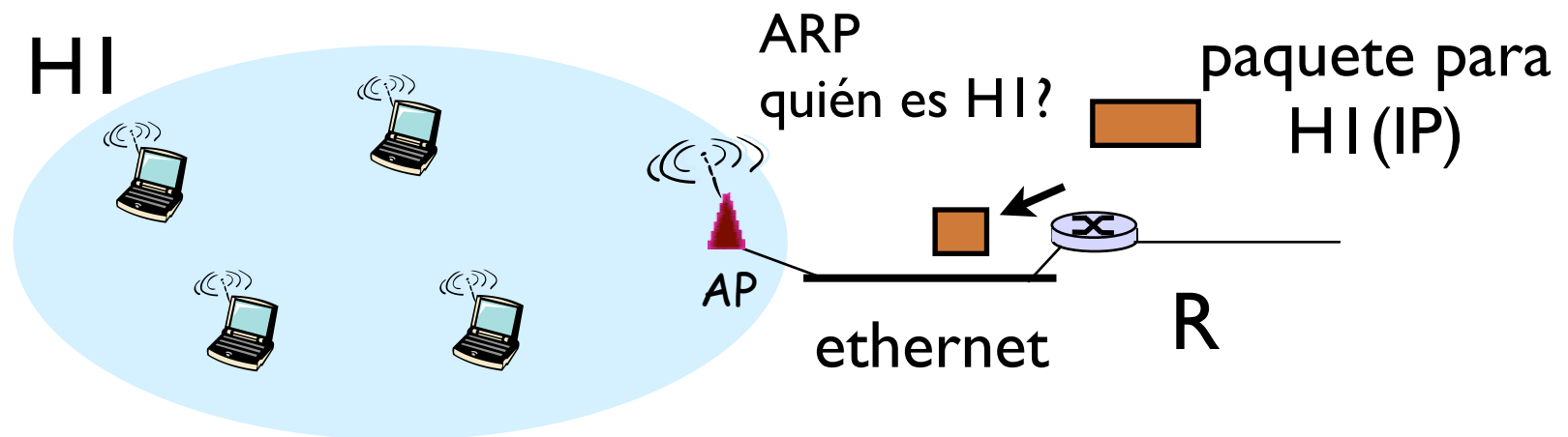
Por qué 3 direcciones?

- ▶ El access point es un dispositivo de nivel de enlace
- ▶ Para los dispositivos conectados al access point no debe haber diferencia entre hosts alámbricos o inalámbricos
- ▶ Como funcionaría el ARP aquí?



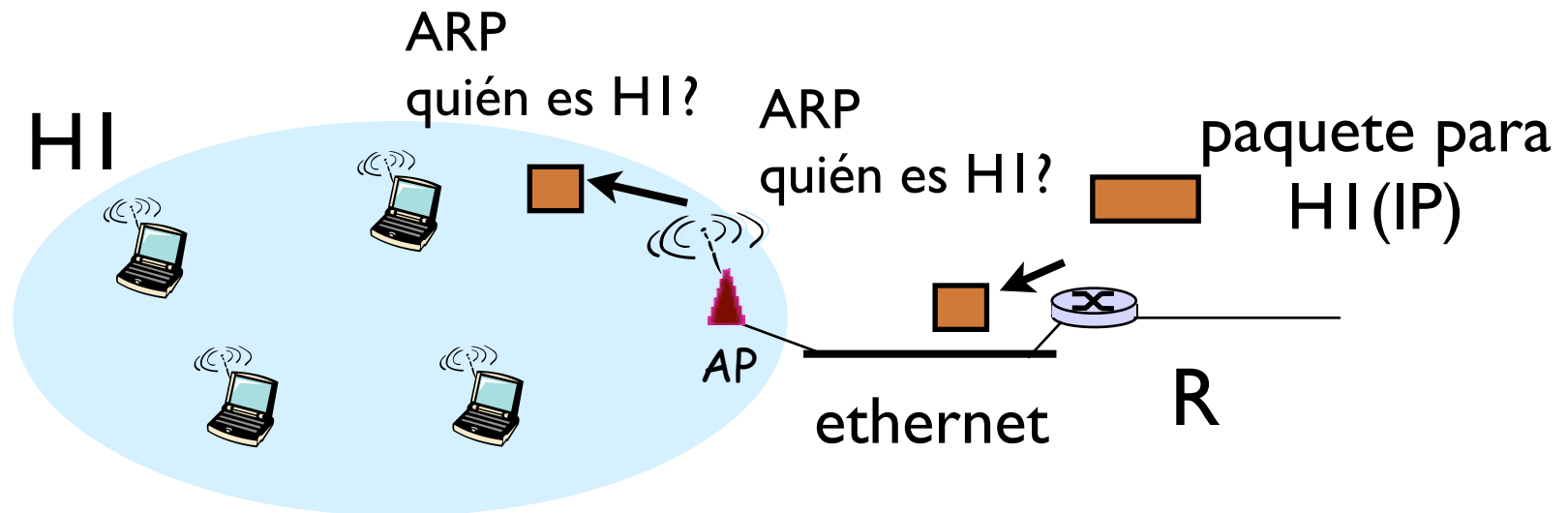
Por qué 3 direcciones?

- ▶ El access point es un dispositivo de nivel de enlace
- ▶ Para los dispositivos conectados al access point no debe haber diferencia entre hosts alámbricos o inalámbricos
- ▶ Como funcionaría el ARP aquí?



Por qué 3 direcciones?

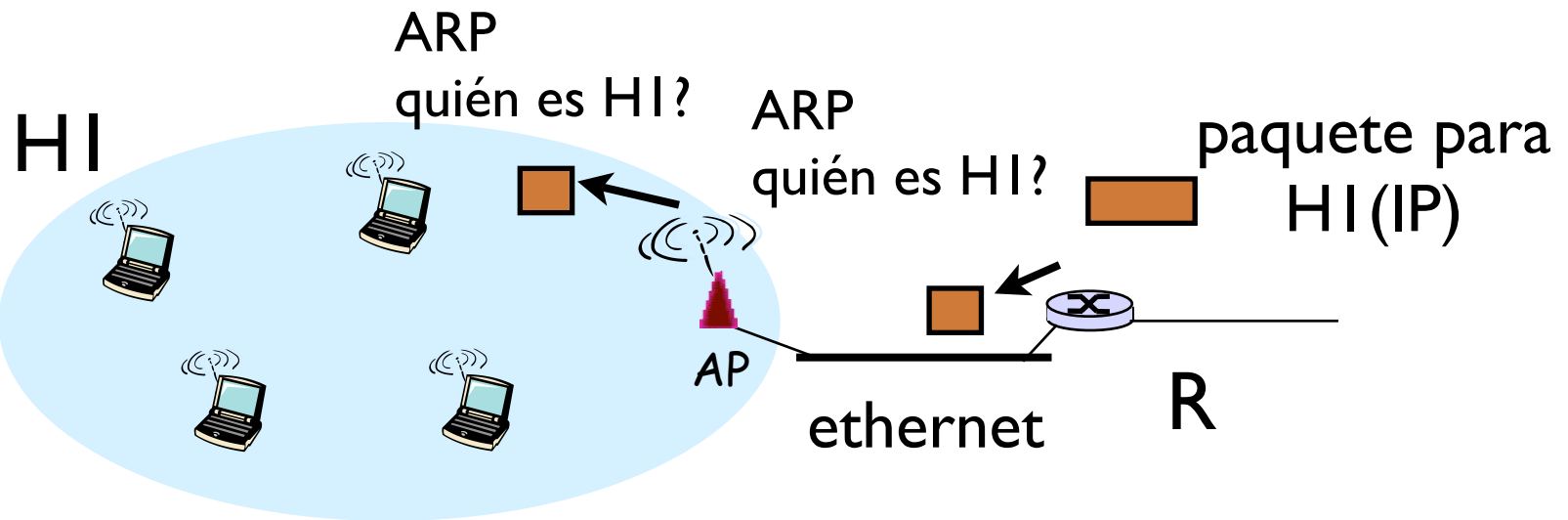
- ▶ El access point es un dispositivo de nivel de enlace
- ▶ Para los dispositivos conectados al access point no debe haber diferencia entre hosts alámbricos o inalámbricos
- ▶ Como funcionaría el ARP aquí?



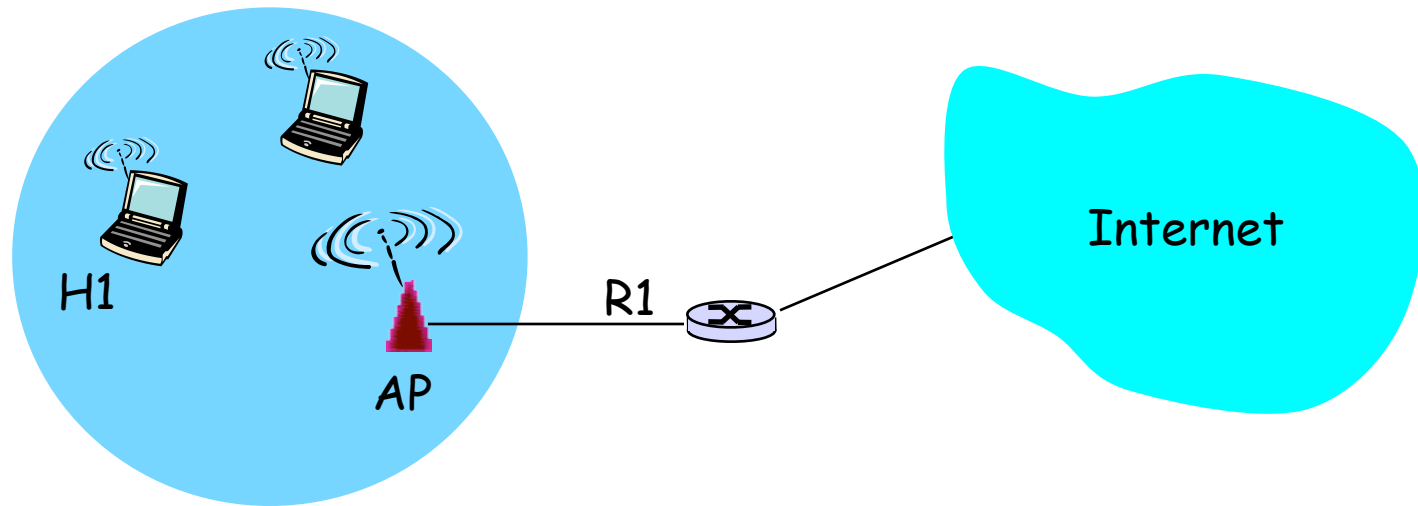
Por qué 3 direcciones?

- ▶ El access point es un dispositivo de nivel de enlace
- ▶ Para los dispositivos conectados al access point no debe haber diferencia entre hosts alámbricos o inalámbricos
- ▶ Como funcionaría el ARP aquí?

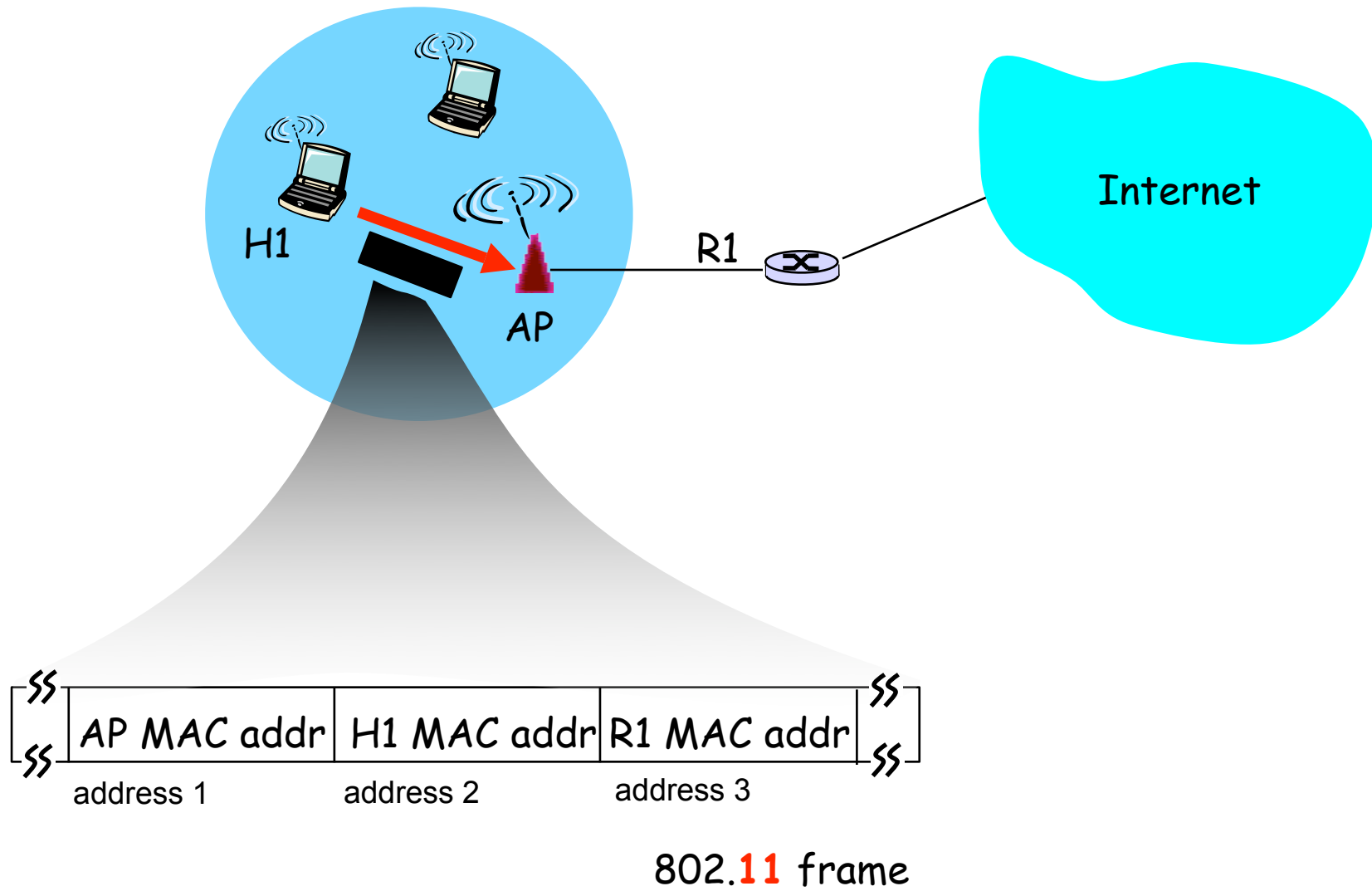
YO
pero
a que MAC
contesto?



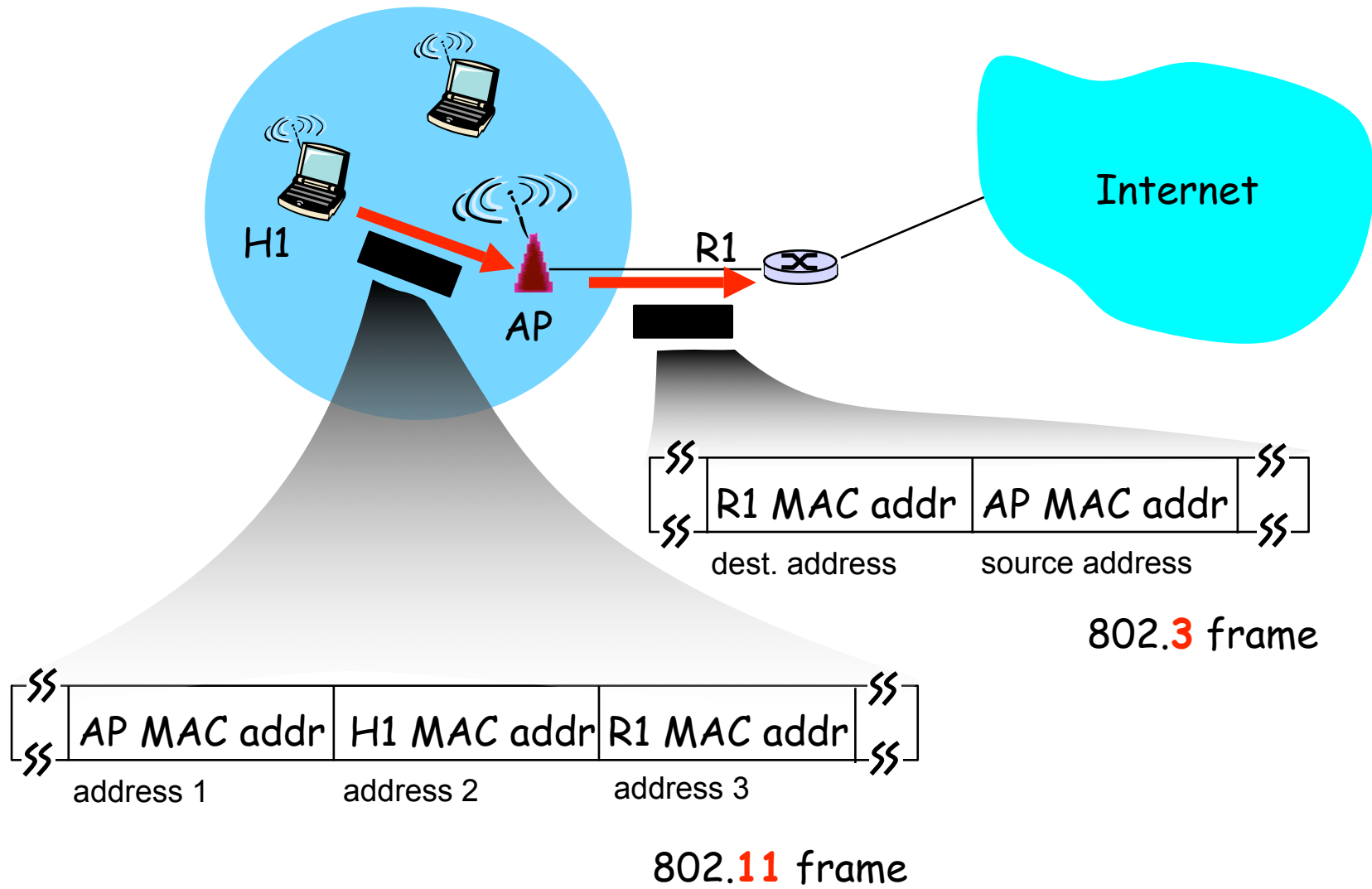
Ejemplo



Ejemplo



Ejemplo



Seguridad en redes 802.11

▶ **Wired Equivalen Privacy (WEP)**

Conseguir en la red inalámbrica el mismo nivel de privacidad que en una de cable

- ▶ Proteger la confidencialidad de los datos que se transmiten por el aire: cifrar las tramas de datos
- ▶ Proteger la integridad de los mensajes

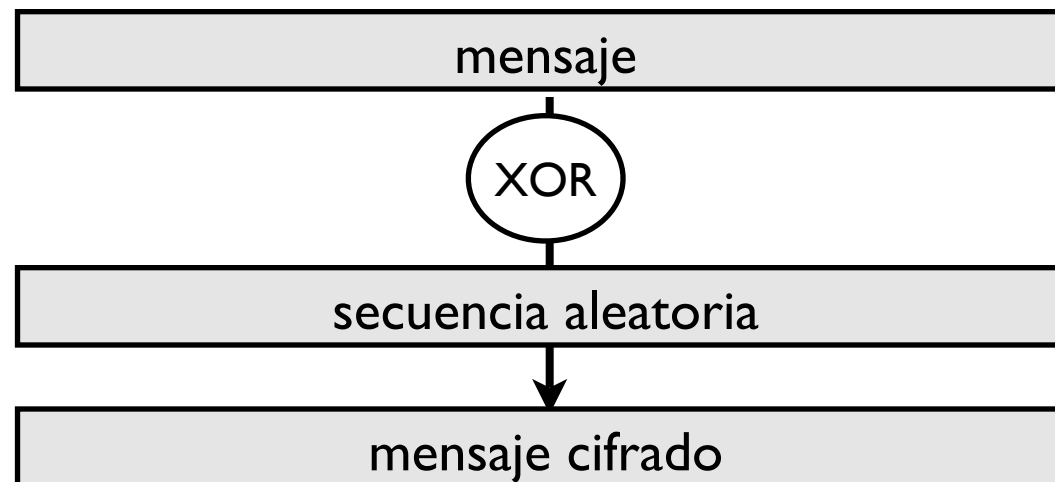
- ▶ Se utiliza el algoritmo de cifrado RC4
 - > Originalmente era un algoritmo propietario de RCA Security
 - > Pero se publicó de forma anónima en Internet y se popularizó
 - El algoritmo cifra a gran velocidad y parecía muy seguro
 - > Con el tiempo se le han ido encontrando algunos problemas...

RC4

- ▶ Rivest Cipher 4 (RC4) Rivest es Ron Rivest la R de RSA
- ▶ Algoritmo de cifrado de tipo clave secreta

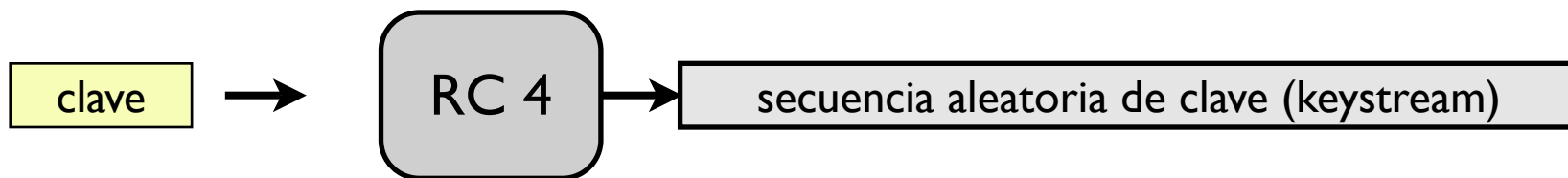
Se basa en generar una serie pseudo-aleatoria a partir de la clave secreta. El mensaje se cifra con una clave de la misma longitud que el mensaje pero que depende de la clave original (intento de hacer un cifrado de Vernan)

- ▶ Cifrado de Vernan cifrar con una secuencia aleatoria tan larga como el mensaje (el destino necesita poder generar la misma secuencia aleatoria)



RC4

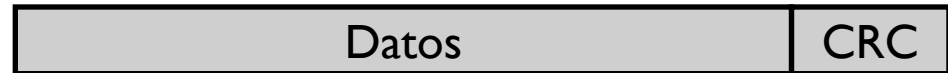
- ▶ Como consigo que origen y destino puedan generar la misma secuencia aleatoria?
 - ▶ Algoritmo RC4 es un generador de secuencia pseudoaleatoria a partir de una semilla de tamaño determinado (256 bytes)
 - ▶ Utilizo como semilla una clave secreta entre emisor y receptor
- Un atacante no puede generar la secuencia sin la semilla



- ▶ Usandolo en WiFi
 - > Para cifrar cada paquete debo empezar de nuevo la secuencia
 - > Demasiado facil de descifrar comparando paquetes
 - > Añadimos una parte variable a la semilla: vector de inicialización (IV)

WEP

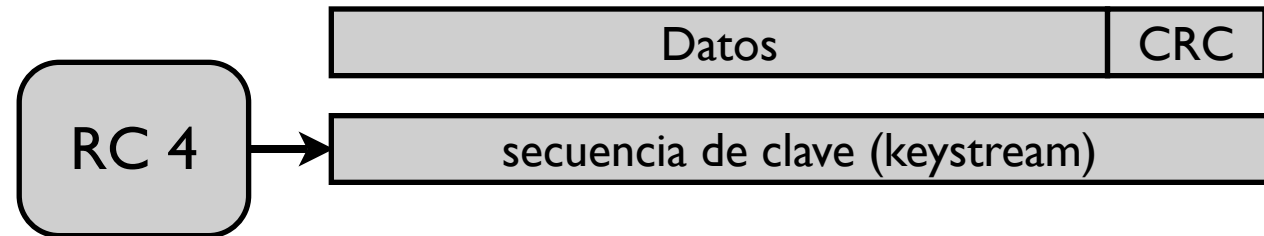
- ▶ A los datos de la trama se les añade un CRC para proteger la integridad y se cifran con RC4



- ▶ Se usan una clave de 64 o 128 bits
 - > Vector de inicialización de 24 bits
 - > Secreto compartido de 40 o 104 bits
- ▶ El vector de inicialización se cambia en cada paquete para cifrar cada paquete con diferente secuencia. Se envía en cada paquete para que el destinatario sea capaz de descifrar.

WEP

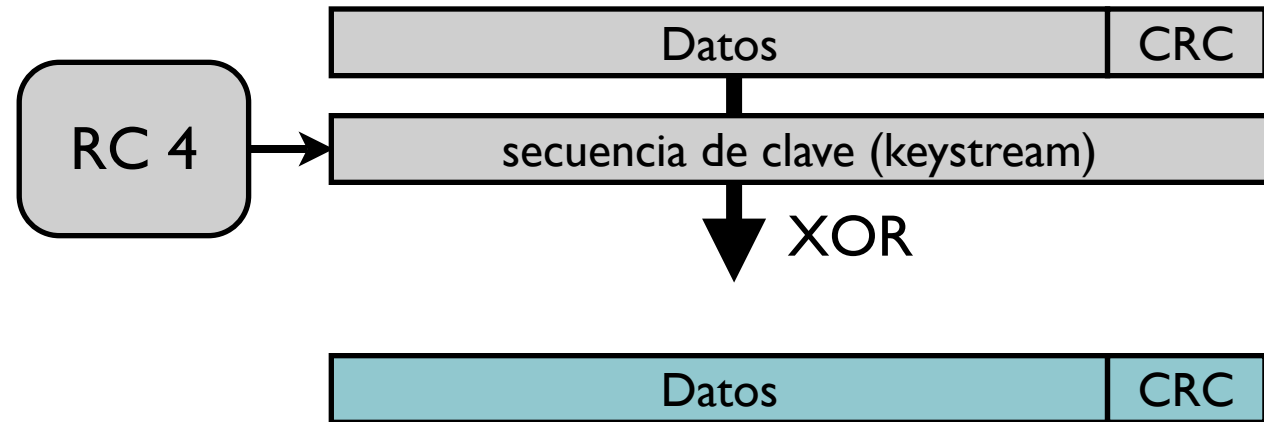
- ▶ A los datos de la trama se les añade un CRC para proteger la integridad y se cifran con RC4



- ▶ Se usan una clave de 64 o 128 bits
 - > Vector de inicialización de 24 bits
 - > Secreto compartido de 40 o 104 bits
- ▶ El vector de inicialización se cambia en cada paquete para cifrar cada paquete con diferente secuencia. Se envía en cada paquete para que el destinatario sea capaz de descifrar.

WEP

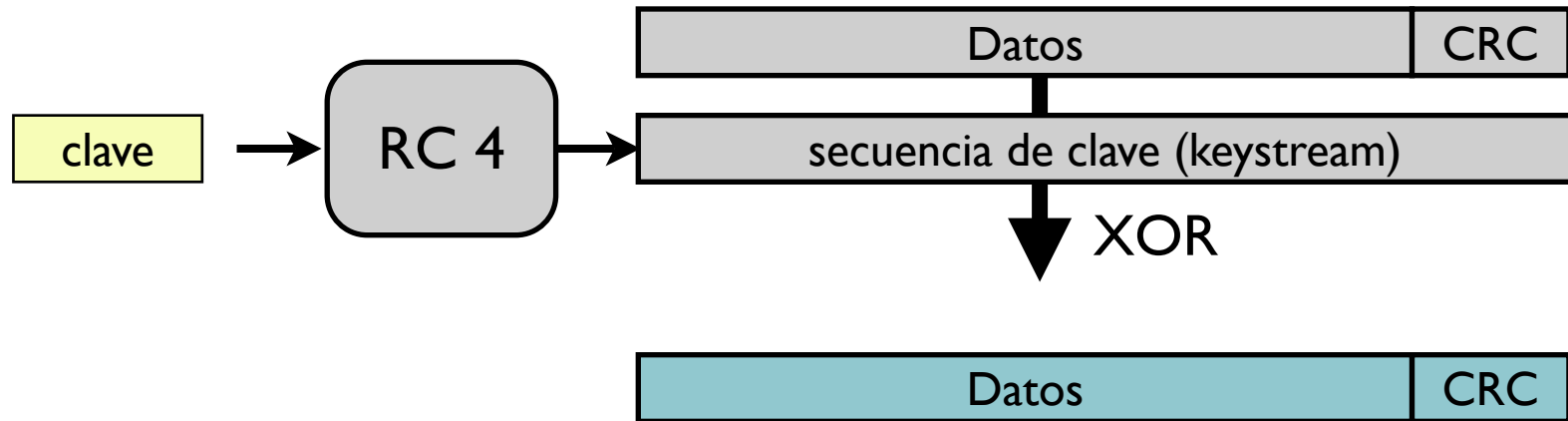
- ▶ A los datos de la trama se les añade un CRC para proteger la integridad y se cifran con RC4



- ▶ Se usan una clave de 64 o 128 bits
 - > Vector de inicialización de 24 bits
 - > Secreto compartido de 40 o 104 bits
- ▶ El vector de inicialización se cambia en cada paquete para cifrar cada paquete con diferente secuencia. Se envía en cada paquete para que el destinatario sea capaz de descifrar.

WEP

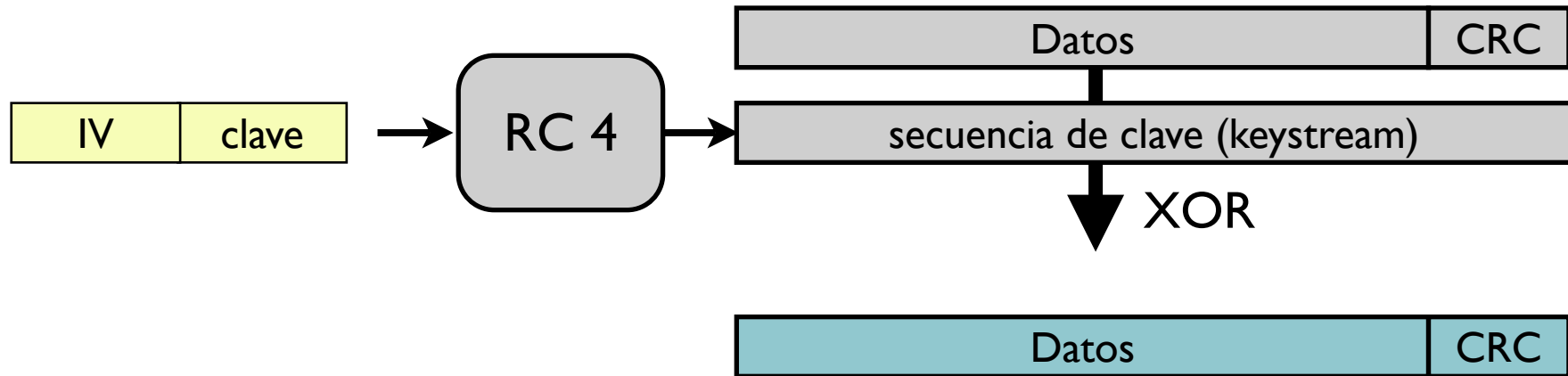
- ▶ A los datos de la trama se les añade un CRC para proteger la integridad y se cifran con RC4



- ▶ Se usan una clave de 64 o 128 bits
 - > Vector de inicialización de 24 bits
 - > Secreto compartido de 40 o 104 bits
- ▶ El vector de inicialización se cambia en cada paquete para cifrar cada paquete con diferente secuencia. Se envía en cada paquete para que el destinatario sea capaz de descifrar.

WEP

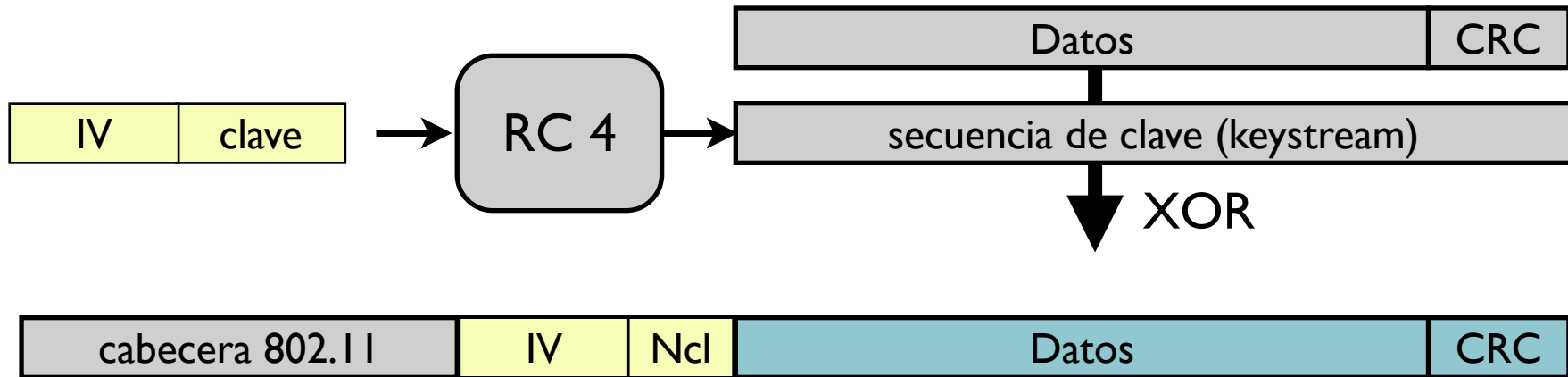
- ▶ A los datos de la trama se les añade un CRC para proteger la integridad y se cifran con RC4



- ▶ Se usan una clave de 64 o 128 bits
 - > Vector de inicialización de 24 bits
 - > Secreto compartido de 40 o 104 bits
- ▶ El vector de inicialización se cambia en cada paquete para cifrar cada paquete con diferente secuencia. Se envía en cada paquete para que el destinatario sea capaz de descifrar.

WEP

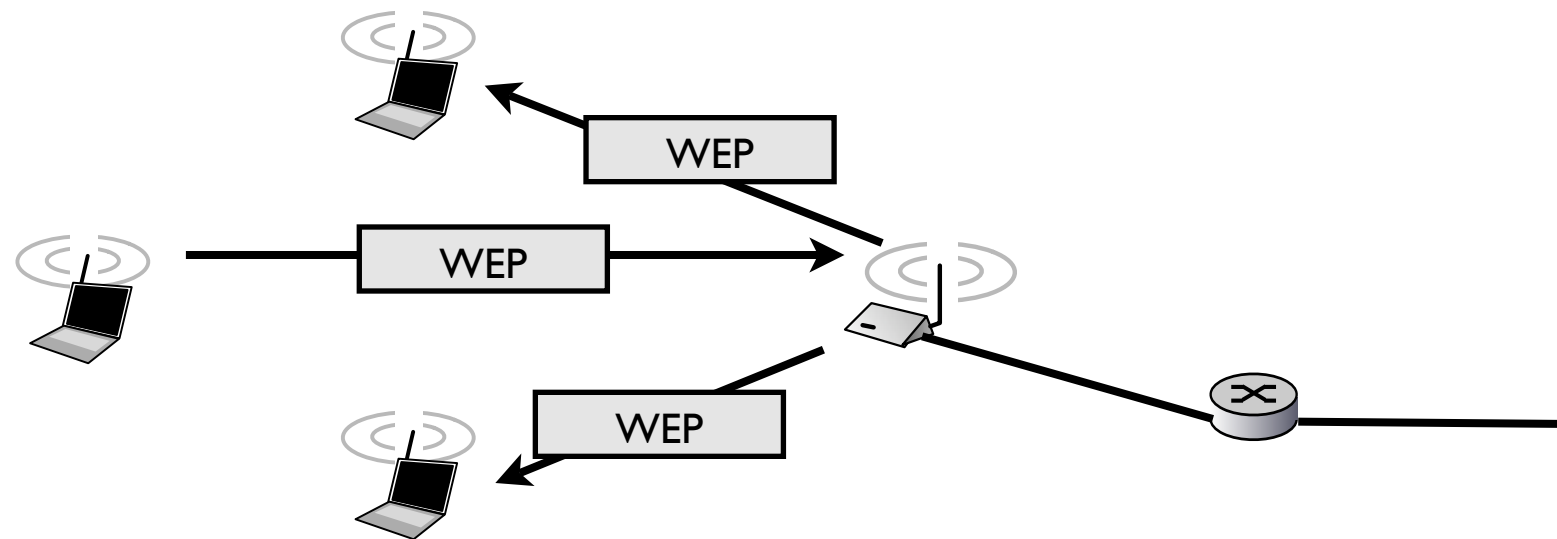
- ▶ A los datos de la trama se les añade un CRC para proteger la integridad y se cifran con RC4



- ▶ Se usan una clave de 64 o 128 bits
 - > Vector de inicialización de 24 bits
 - > Secreto compartido de 40 o 104 bits
- ▶ El vector de inicialización se cambia en cada paquete para cifrar cada paquete con diferente secuencia. Se envía en cada paquete para que el destinatario sea capaz de descifrar.

WEP

- ▶ Enviando con WEP
 - > El terminal calcula el CRC del paquete y cifra el paquete con WEP
 - > El paquete se envía al access point
 - > El access point descifra el paquete y si el CRC es inválido lo tira
 - > El access point puede cifrarlo con otro IV y enviarlo



- ▶ Un intruso
 - > No puede descifrar los paquetes que le llegan
 - > No puede generar paquetes válidos para otros

Ventajas

- ▶ Autenticación sencilla: los usuarios que conozcan la clave pueden usar la red inalámbrica
- ▶ Protección de integridad y confidencialidad “razonable”
 - > o no?

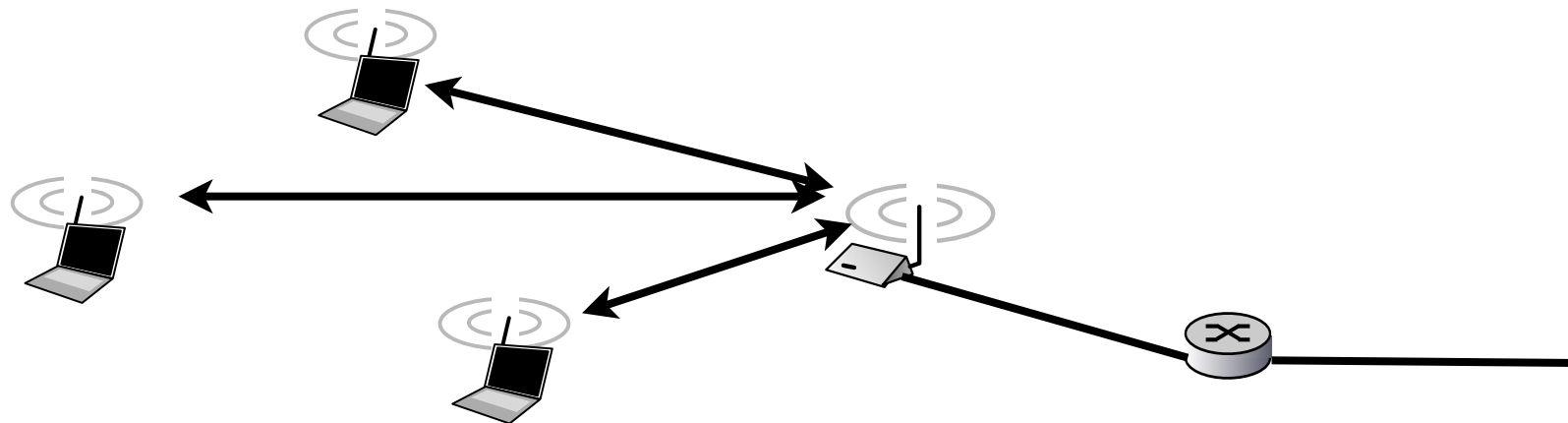
Seguridad en WiFi (escenarios)

- ▶ Opción I: Red wifi abierta

SSID se anuncia

Autenticación abierta (se autoriza a todo el que lo pide)

No hay encriptación (WEP desactivado)



Seguridad en WiFi (escenarios)

▶ Opción 2: Red wifi con WEP

SSID se anuncia

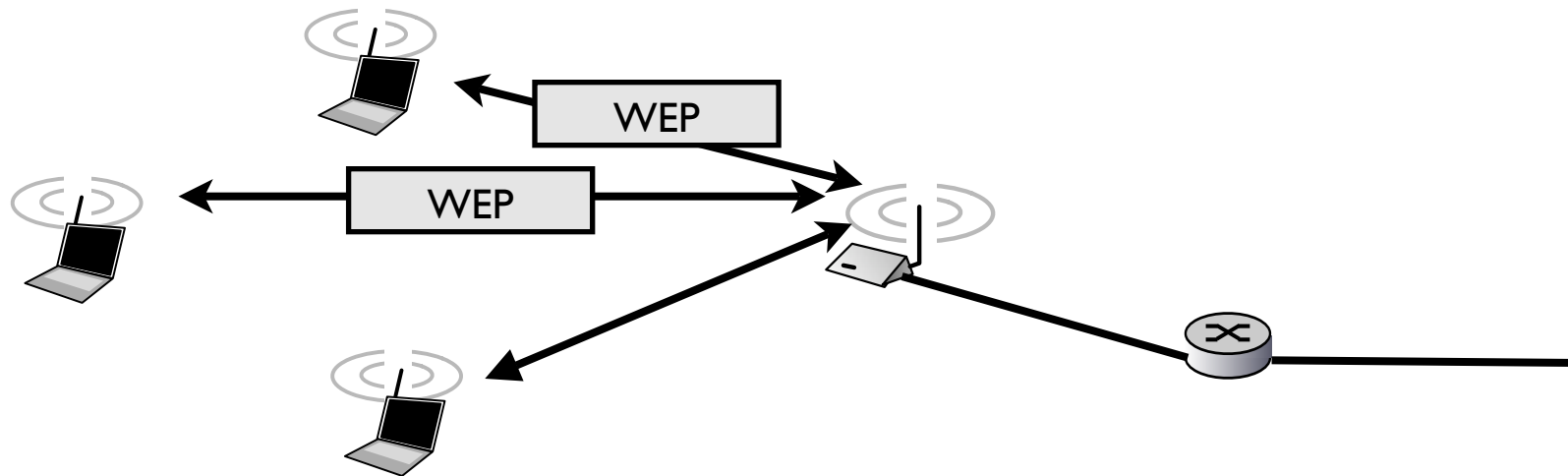
Se puede ocultar el SSID pero un sniffer puede verlo en las tramas de autenticación/ asociación de los usuarios autorizados

Autenticación abierta (se autoriza a todo el que lo pide)

Se puede poner autenticación SKA pero se considera que disminuye la seguridad

Hay encriptación WEP

Solo los que conozcan la clave pueden enviar/recibir



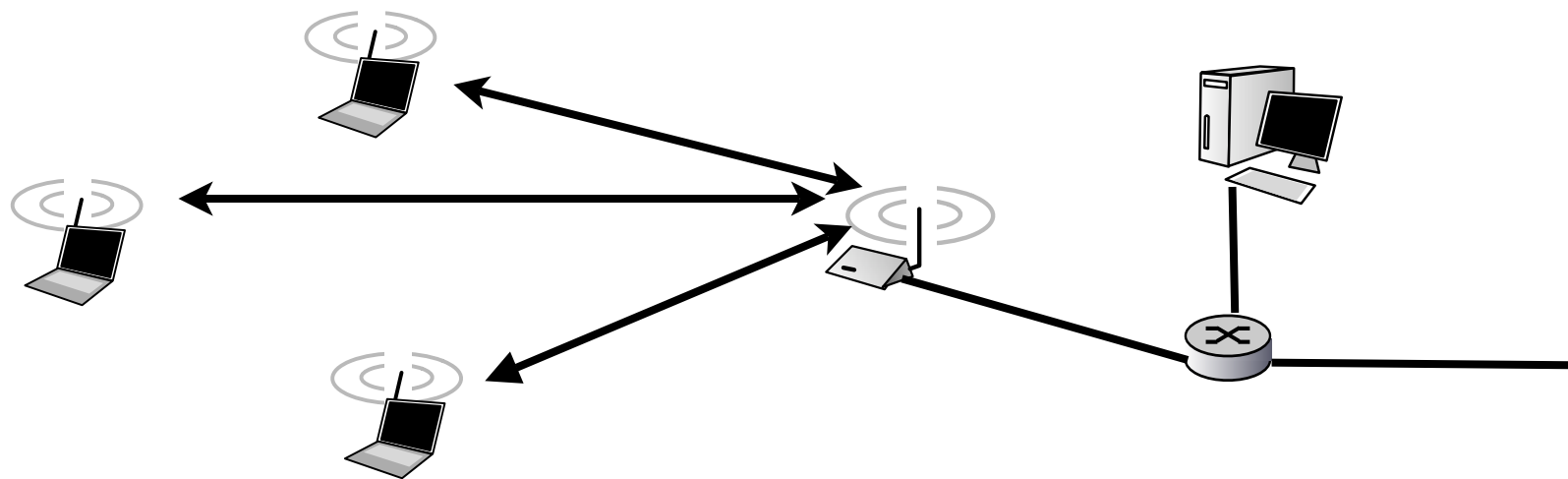
Seguridad en WiFi (escenarios)

- ▶ Opción 3: otros...

SSID se anuncia

Autenticación abierta (se autoriza a todo el que lo pide)

No hay encriptación (WEP desactivado)



- ▶ Autenticación via Web por el usuario

- > En el router de salida se corta el acceso a direcciones MAC o IP