



# Tema 6. Nivel de enlace

Introducción a las redes de ordenadores

Boni García  
Curso 2017/2018

# Índice de contenidos

---

1. Introducción al nivel de enlace
2. Ethernet
3. Wifi

# Índice de contenidos

---

1. Introducción al nivel de enlace
2. Ethernet
3. Wifi

# 1. Introducción al nivel de enlace

---

- El nivel de enlace proporciona comunicación entre dos máquinas que están conectadas directamente (segmento de red)
- El nivel de enlace está implementado en el adaptador de red, que normalmente es hardware
- Las entidades involucradas en una comunicación a nivel de enlace se denominan:
  - DTE (*Data Terminal Equipment*): Dispositivos que generan datos (estaciones finales). Normalmente serán estaciones de trabajo, servidores de archivos/impresión, etc.
  - DCE (*Data Circuit-terminating Equipment*): Dispositivos que reciben datos y los retransmiten dentro de la red. No son por tanto ni los emisores originales ni los receptores finales de la comunicación, sino equipos intermedios entre los extremos de la comunicación final

# 1. Introducción al nivel de enlace

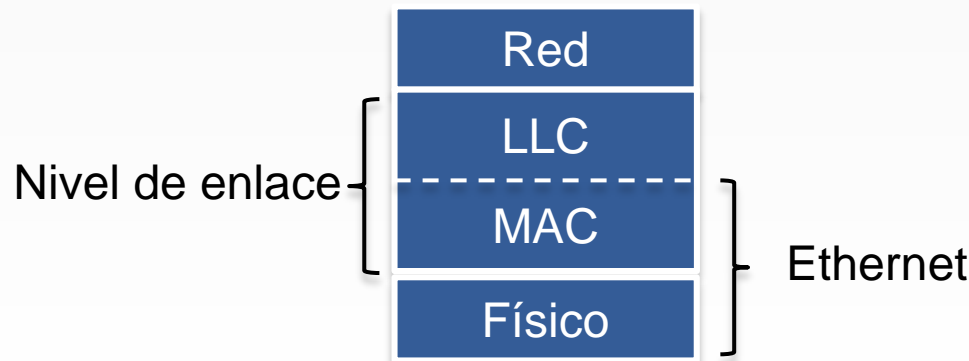
---

- Servicios posibles proporcionados por el nivel de enlace:
  - *Framing*: Todos los protocolos de enlace proporcionan la encapsulación de datos en tramas
  - Acceso al enlace: Reglas de acceso al medio físico
  - Transporte fiable: Entre los extremos del enlace
  - Control de flujo: No sobrepasar la capacidad de buffer de recepción
  - Detección de errores (a nivel de bits)
  - Corrección de errores

# 1. Introducción al nivel de enlace

---

- El nivel de enlace está dividido conceptualmente en dos subniveles:
  - Control de Enlace Lógico (LLC, *Link Layer Control*). La subcapa LLC maneja funciones como el control de errores y control del flujo. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientado a conexión y orientadas a conexión
  - Control de Acceso al Medio (MAC, *Media Access Control*). La subcapa MAC define los procedimientos usados para acceder al medio compartido



# Índice de contenidos

---

1. Introducción al nivel de enlace
2. Ethernet
  - Historia de Ethernet
  - Estructura de la trama IEEE 802.3
  - Mecanismo de acceso al medio
  - Tecnologías Ethernet
  - ARP
3. Wifi

## 2. Ethernet

- **Ethernet** es la tecnología predominante para el nivel de enlace y físico en el modelo Internet
- Ethernet opera en la subcapa MAC así como en la capa física pero no en la subcapa LLC
- Ethernet está estandarizado en la familia de estándares **IEEE 802.3** (protocolos no orientado a conexión)
- La topología lógica de las redes Ethernet es en **bus**
  - Típicamente la interconexión física será en estrella (switch como punto central), pero a nivel lógico todos los equipos comparten el mismo canal





## 2. Ethernet

---

### Historia de Ethernet

- Ethernet fue creado en 1973 por Robert Metcalfe en la empresa Xerox
- El nombre “Ethernet” hacía referencia a la teoría de la física hoy ya abandonada según la cual las ondas electromagnéticas viajaban por un fluido denominado éter que se suponía llenaba todo el espacio
- Para Metcalfe el 'éter' era el cable coaxial por el que iba la señal
- Los ordenadores Xerox utilizados para las primeras pruebas de Ethernet fueron rebautizadas con los nombres Michelson y Morley (nombre de los físicos responsables del primer experimento que demostró la no existencia del éter)
- En 1982 el consorcio DIX (Digital Equipment Corporation, Intel, Xerox) publicaron el estándar Ethernet II, que es la base de la familia de estándares internacionales IEEE 802.3

## 2. Ethernet

### Estructura de la trama IEEE 802.3

Preámbulo	SFD	MAC origen	MAC destino	EtherType/ Longitud	Datos	CRC	IFG
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes	12 bytes

Trama Ethernet a nivel 2 (enlace)

Trama Ethernet a nivel 1 (físico)

- Preámbulo: Palabra binaria usada para sincronización a nivel físico
- SFD (*Start Frame Delimiter*): Palabra binaria diferente al preámbulo que delimita el inicio de la trama a nivel de enlace
- IFG (*Inter Frame Gap*): Tiempo correspondiente a 96 bits que un host debe esperar antes de enviar otra trama

## 2. Ethernet

### Estructura de la trama IEEE 802.3

- Direcciones MAC destino y origen
  - Longitud: 6 bytes (48 bits)
  - Cada tarjeta de red (NIC, *Network Interface Card*) tiene una dirección MAC única (administradas por el IEEE)
  - Los tres primeros bytes de cada dirección MAC son propios del fabricante
  - Dirección broadcast: FF-FF-FF-FF-FF-FF
- Tipo/Longitud (2 bytes)
  - La mayoría de tarjetas de red Ethernet usan este campo siguiendo la especificación inicial de Ethernet (DIX Ethernet II) con lo que estos 2 bytes determinan el **tipo** de protocolo encapsulado en el campo de datos de la trama
  - Si el valor de este campo  $\leq 1500$ , entonces determina la longitud de la cabecera LLC contenida en el campo datos

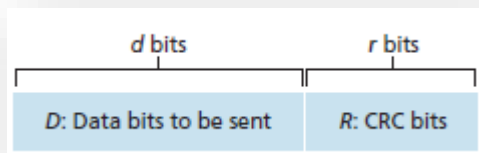


EtherType	Datos
0x0800	IPv4
0x86DD	IPv6
0x0806	ARP

## 2. Ethernet

### Estructura de la trama IEEE 802.3

- Payload: Datos mínimo 46 bytes, máximo de 1500 Bytes → MTU (*Maximum Transfer Unit*)
- CRC (4 bytes). Código de redundancia cíclica. También llamado FCS (*Frame Check Sequence*)
  - El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor recalcula para comprobar si la trama es válida



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

$$G_{CRC-32} = 0x104C11DB7$$

## 2. Ethernet

---

### CSMA/CD

- El mecanismo de acceso al medio implementado en Ethernet se conoce como **CSMA/CD** (Acceso Múltiple por Detección de Portadora con Detección de Colisiones)
- El mecanismo de funcionamiento es equivalente a una conversación en una habitación oscura:
  - Antes de hablar, todo el mundo escucha hasta que se produce un periodo de silencio (CS, detección de portadora)
  - Una vez que hay silencio, todo el mundo tiene las mismas oportunidades de decir algo (MA, acceso múltiple)
  - Si dos personas empiezan a hablar al mismo tiempo, se dan cuenta de ello y dejan de hablar (CD, detección de colisiones)

## 2. Ethernet

---

### CSMA/CD

- Cada host que desea transmitir debe realizar una escucha del medio (detección de portadora) para comprobar si éste se encuentra libre
- Si el medio se encuentra libre entonces el host puede transmitir
- Puede ocurrir que varios host comiencen a transmitir una trama en el mismo instante. Cuando esto se sucede, se dice que ha ocurrido una **colisión**
- La estación que ha detectado la colisión procederá a enviar un mensaje de *jam* de 32 bits al resto de estaciones para notificar la detección de colisión
- Al recibir este mensaje se paran todas las transmisiones y se ejecuta un algoritmo de espera antes de volver a intentar la transmisión
  - Durante los 10 primeros intentos el valor medio del tiempo de espera se duplica mientras que durante los 6 siguientes intentos adicionales, se mantiene
  - Tras 16 intentos fallidos, el algoritmo notificará un error a las capas superiores

## 2. Ethernet

---

### Tecnologías Ethernet

- Existen diferentes estándares Ethernet: la familia de protocolos IEEE 802.3
- Estos protocolos se diferencian en: velocidad de transmisión, tipo de medio físico, longitud máxima, y topología de red
- La notación de las diferentes tecnologías Ethernet sigue la siguiente notación:
  1. Velocidad de transmisión: en Mbps (o en Gbps si va precedido del sufijo “G”)
  2. Tipo de transmisión: BASE=banda base, BROAD=banda ancha (no usado en ninguna implementación actual)
  3. Distinción adicional:
    - Longitud de bus x 100 metros
    - Tipo de medio: T=Par de cobre trenzado; F=Fibra óptica; C=Par de cobre trenzado apantallando; S,L,E=Infrarrojo cercano (laser de 850, 1310, y 1550 nm respectivamente)

## 2. Ethernet

### Tecnologías Ethernet

Familia	Tecnología	Velocidad	Medio de transmisión	Distancia
Ethernet	10BASE-5	10 Mbps	Coaxial	500 m
	10BASE-2	10 Mbps	Coaxial	185 m
	10BASE-T	10 Mbps	Par trenzado	100 m
	10BASE-F	10 Mbps	Fibra óptica	2000 m
Fast Ethernet	100BASE-TX	100 Mbps	Par trenzado	100 m
	100BASE-FX	100 Mbps	Fibra óptica	2000 m
Gigabit Ethernet	1000BASE-T	1 Gbps	Par trenzado	100 m
	1000BASE-CX	1 Gbps	Par trenzado apantallado	25 m

- Las siguientes familias son 10 Gigabit Ethernet, 40 Gigabit Ethernet y 100 Gigabit Ethernet (velocidades de 10, 40, 100 Gbps respectivamente)



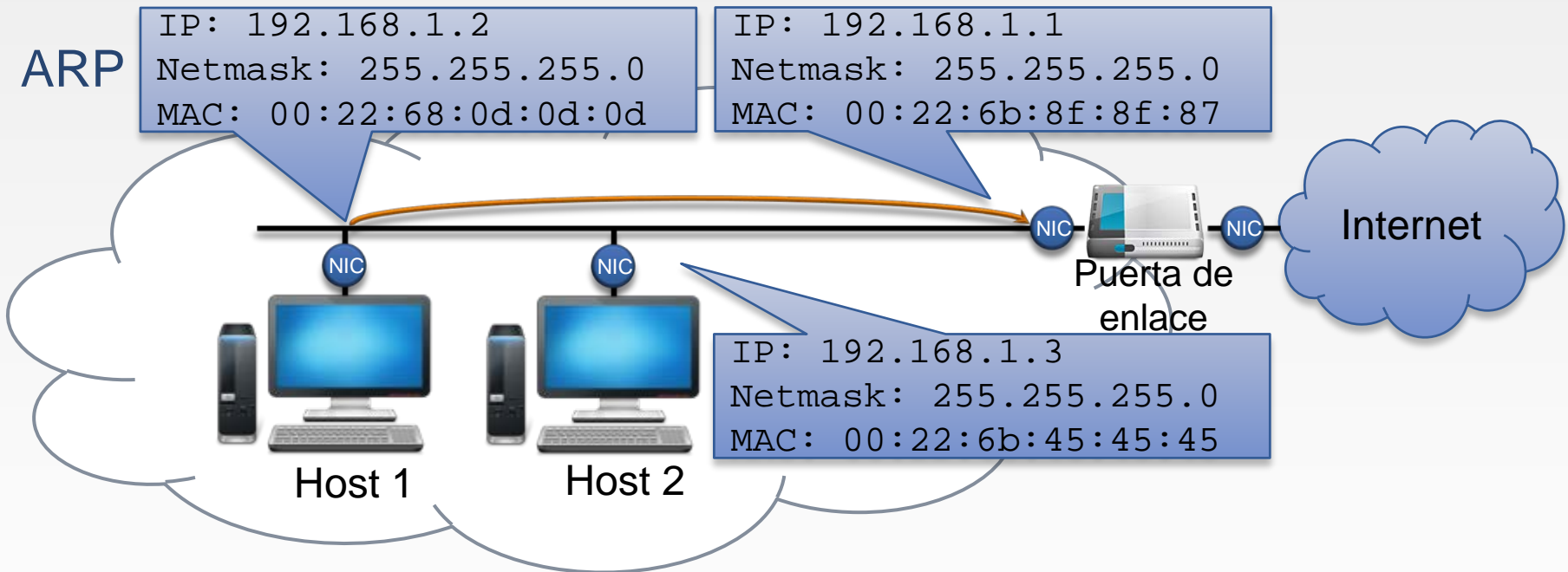
## 2. Ethernet

---

### ARP

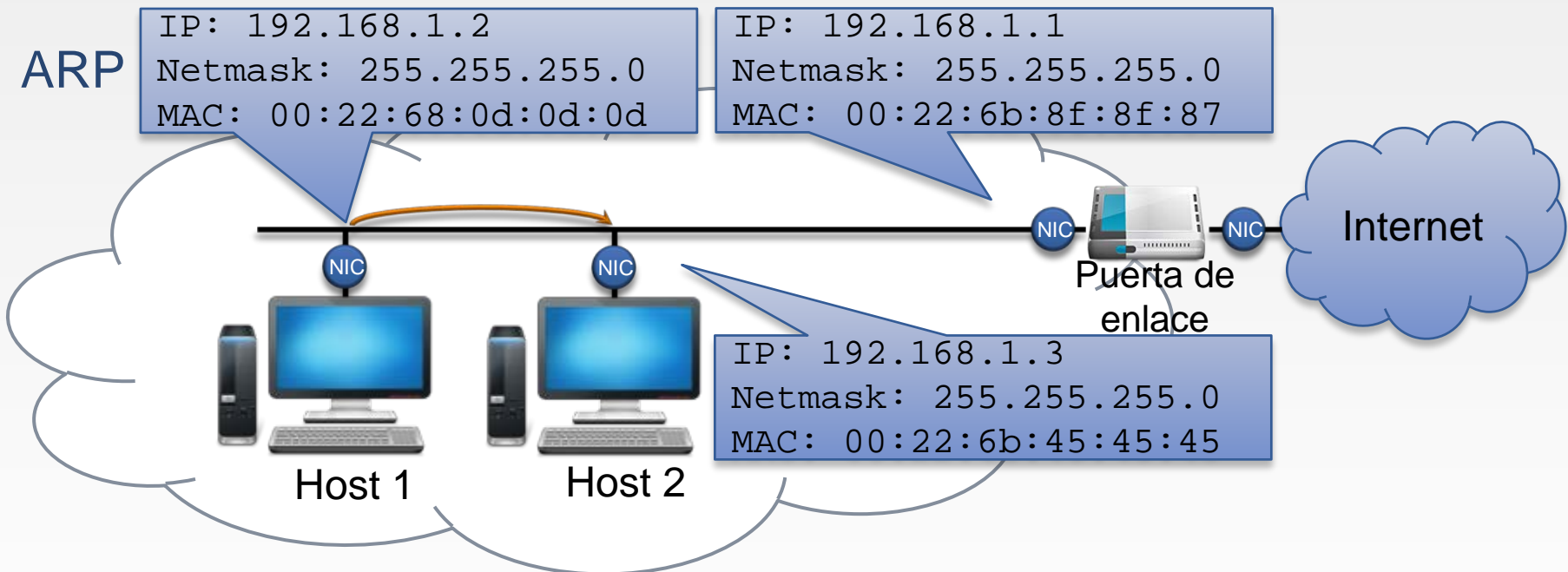
- Un host que quiere enviar un paquete IP debe conocer la IP destino
- Mediante esa IP destino, el host origen podrá averiguar si el host destino está en la red local o no, mediante el siguiente calculo:
  1. Si prefijo de red = prefijo de red destino → IP destino está en la misma red
  2. Si prefijo de red ≠ prefijo de red destino → IP destino no está en la misma red
- El prefijo de red se calcula mediante la operación binaria AND:  
prefijo de red = IP local · máscara de red
- En el caso **1** (IP destino en la misma red) el paquete IP se encapsulará en una trama dirigida directamente al **host destino**
- En el caso **2** (IP destino en la misma red) el paquete IP se encapsulará en una trama dirigida a la **puerta de enlace** (que proporciona conectividad con el exterior de la red)

## 2. Ethernet



- Ejemplo 1: IP destino= **216.58.210.227**  
 Prefijo de red =  $192.168.1.2 \cdot 255.255.255.0 = 192.168.1.0$   
 Prefijo de red destino =  $216.58.210.227 \cdot 255.255.255.0 = 216.58.210.0$   
 $192.168.1.0 \neq 0 \ 216.58.210.0 \rightarrow$  No están en la misma red  
 $\rightarrow$  Se creará una trama dirigida a la **puerta de enlace**

## 2. Ethernet



- Ejemplo 2: IP destino= **192.168.1.3**  
 Prefijo de red =  $192.168.1.2 \cdot 255.255.255.0 = 192.168.1.0$   
 Prefijo de red destino =  $192.168.1.3 \cdot 255.255.255.0 = 192.168.1.0$   
 $192.168.1.0 = 192.168.1.0 \rightarrow$  Sí están en la misma red  
 $\rightarrow$  Se creará una trama dirigida al **host 2**

## 2. Ethernet

---

### ARP

- ARP (*Address Resolution Protocol*) es un protocolo de nivel de enlace que sirve para encontrar la dirección IP de una determina dirección MAC
- Hay dos tipos de mensajes ARP:
  - *Request* (campo *operation code* = 1)
    - ¿Quién tiene la IP x.x.x.x?
    - Se envían por la dirección MAC broadcast (FF-FF-FF-FF-FF-FF)
  - *Reply* (campo *operation code* = 0)
    - Responderá únicamente el poseedor de esa IP
- Esta información se guarda en la **tabla ARP**:
  - Dirección IP
  - Dirección MAC
  - Tipo de asociación
    - Dinámico: entrada creada como respuesta a una petición
    - Estático: entrada creada manualmente

## 2. Ethernet

---

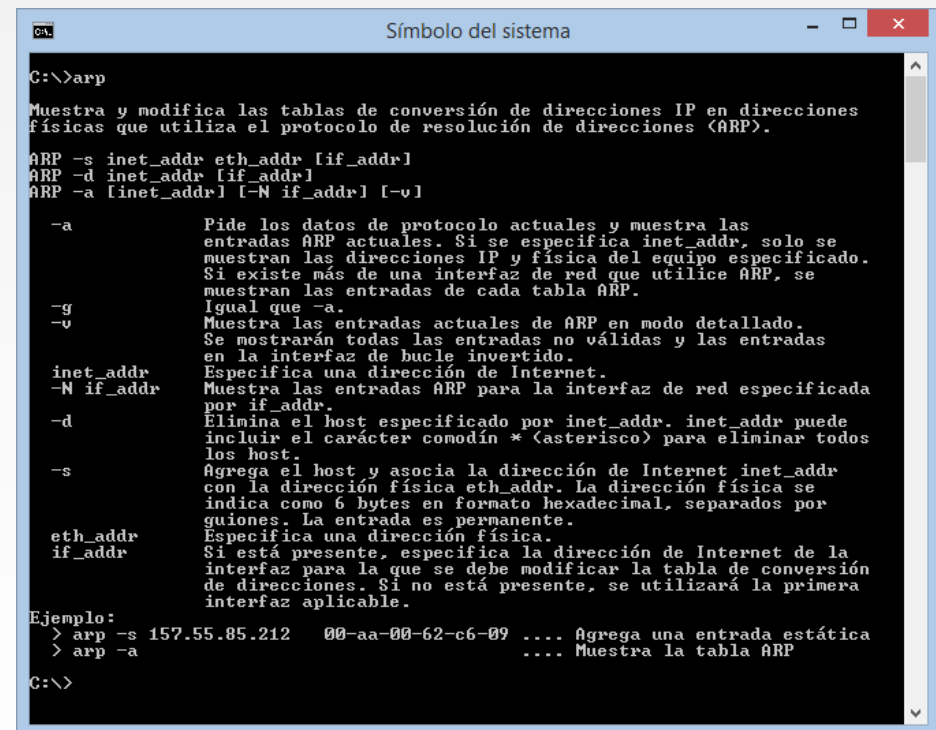
### ARP

- ARP gratuito: al inicializar una interfaz, una entidad de red manda ARP request para anunciar su dirección IP, y así el resto actualice su tabla ARP
- ARP también puede usarse para preguntar por la dirección IP propia, de forma que una máquina puede detectar conflictos con otros nodos con su misma dirección IP (en caso de recibir respuesta)
- ¿Es segura la tabla ARP? No. La tabla ARP se puede envenenar realizando un ataque denominado *ARP Spoofing*
  - Consiste en inundar la red con mensajes ARP indicando que la MAC de la “víctima” y de la puerta de enlace (router) pertenecen al usuario malicioso
  - Las máquinas actualizan sus tablas ARP
  - Las tramas de la víctima al router serán interceptadas por el usuario malicioso, que reenviará los paquetes a su verdadero destinatario (*man-in-the-middle*)

## 2. Ethernet

### ARP

- `arp -a`
  - Para mostrar la tabla ARP
- `arp -d *`
  - Para borrar la tabla ARP
  - Este comando tiene que se ejecutado como administrador/root
- `arp -s IP MAC`
  - Para añadir una entrada estática



```
C:\>arp

Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a           Pide los datos de protocolo actuales y muestra las
             entradas ARP actuales. Si se especifica inet_addr, solo se
             muestran las direcciones IP y física del equipo especificado.
             Si existe más de una interfaz de red que utilice ARP, se
             muestran las entradas de cada tabla ARP.
-g           Igual que -a.
-v           Muestra las entradas actuales de ARP en modo detallado.
             Se mostrarán todas las entradas no válidas y las entradas
             en la interfaz de bucle invertido.
inet_addr    Especifica una dirección de Internet.
-N if_addr   Muestra las entradas ARP para la interfaz de red especificada
             por if_addr.
-d           Elimina el host especificado por inet_addr. inet_addr puede
             incluir el carácter comodín * (asterisco) para eliminar todos
             los host.
-s           Agrega el host y asocia la dirección de Internet inet_addr
             con la dirección física eth_addr. La dirección física se
             indica como 6 bytes en formato hexadecimal, separados por
             guiones. La entrada es permanente.
eth_addr     Especifica una dirección física.
if_addr      Si está presente, especifica la dirección de Internet de la
             interfaz para la que se debe modificar la tabla de conversión
             de direcciones. Si no está presente, se utilizará la primera
             interfaz aplicable.

Ejemplo:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Agrega una entrada estática
> arp -a .... Muestra la tabla ARP

C:\>
```

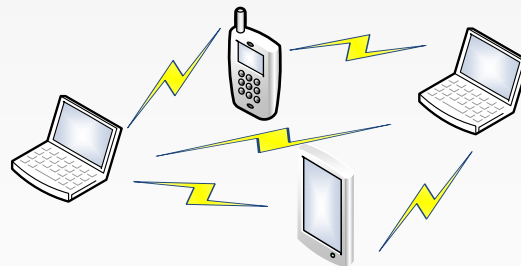
# Índice de contenidos

---

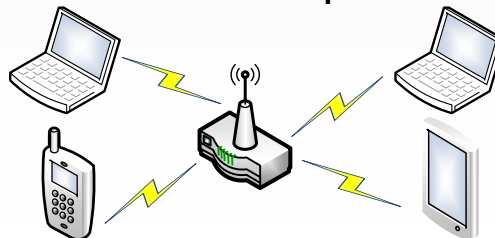
1. Introducción al nivel de enlace
2. Ethernet
3. Wifi
  - Estándares IEEE 802.11
  - Punto de acceso
  - Seguridad
  - Técnica de transmisión
  - Otras tecnologías inalámbricas

## 3. Wifi

- Las redes locales inalámbricas (*Wireless LAN, WLAN*) permiten la interconexión de hosts en área local sin necesidad de usar cables
- Las WLAN pueden utilizarse de dos formas:
  - Para establecer **redes ad-hoc**, esto es, redes cerradas donde un grupo de terminales próximos se comunican entre sí sin acceso a redes externas



- Como **redes de acceso inalámbricas**, donde los terminales se comunican con un punto de acceso a través del cual pueden interconectarse entre sí y acceder a redes externas





## 3. Wifi

---

- La tecnología WLAN más utilizada en redes inalámbricas es el **wifi**. Según la RAE:

**wifi**

Tb. **wi fi**.

Del ingl. *Wi-Fi*®, marca reg.

1. m. *Inform.* Sistema de conexión inalámbrica, dentro de un área determinada, entre dispositivos electrónicos, y frecuentemente para acceso a internet. U. t. en apos., y t. c. f.

*Real Academia Española © Todos los derechos reservados*

- Wi-Fi es una marca registrada de la Wi-Fi Alliance, la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares **IEEE 802.11**



## 3. Wifi

---

### Historia

- En 1999 se creó la empresa **WECA** (*Wireless Ethernet Compatibility Alliance*) por Nokia y Symbols Technologies
- El objetivo de WECA era de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma **IEEE 802.11**
- En 2002 WECA cambió de nombre, pasando a llamarse **Wi-Fi Alliance**
- “Wi-Fi” es un nombre comercial, creado para ser corto y fácil de recordar
  - Su similitud con Hi-Fi (*High Fidelity*) ha crear erróneamente que proviene de *Wireless Fidelity*
- La familia de estándares IEEE 802.11 definen el uso de los niveles de enlace y físico en una WLAN

## 3. Wifi

---

### Estándares IEEE 802.11

- Las redes 802.11 (Wi-Fi) siguen en líneas generales lo dispuesto en el 802.3 (Ethernet)
  - Emplean un mecanismo de acceso al medio basado en CSMA (*Carrier Sense Medium Access*, detección de portadora y acceso al medio)
  - Necesitan una capa física (PHY) y de acceso al medio (MAC) específicas para poder utilizar el espectro radioeléctrico
  - Tienen una dirección física **MAC** de 64 bits
- Las redes 802.11 utilizan principalmente bandas de frecuencias **ISM** (*Industrial, Scientific and Medical*)
  - Son bandas reservadas internacionalmente para uso no comercial
  - Pueden utilizarse sin necesidad de licencia siempre que se respeten unos límites de potencia (en España la potencia máxima permitida de emisión para la banda ISM de 2,4GHz es de 100mW)

## 3. Wifi

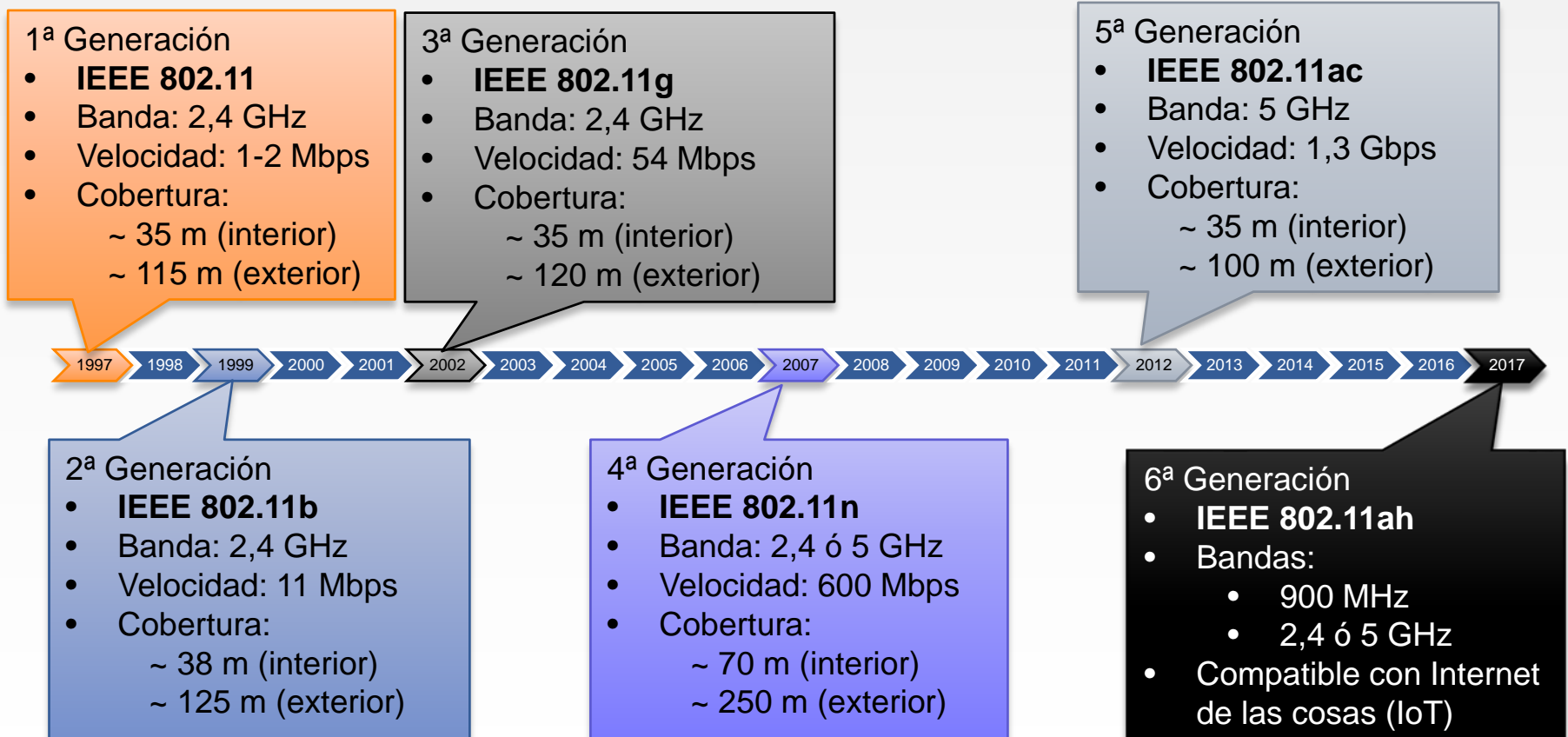
### Estándares IEEE 802.11

- Las bandas **ISM** mundiales definidas por el ITU-R son:

Rango de frecuencias		Ancho de banda	Frecuencia central
13,553 MHz	13,567 MHz	14 kHz	13,560 MHz
26,957 MHz	27,283 MHz	326 kHz	27,120 MHz
40,660 MHz	40,700 MHz	40 kHz	40,680 MHz
2,400 GHz	2,500 GHz	100 MHz	2,450 GHz
5,725 GHz	5,875 GHz	150 MHz	5,800 GHz
24,000 GHz	24,250 GHz	250 MHz	24,125 GHz

## 3. Wifi

### Estándares IEEE 802.11



## 3. Wifi

---

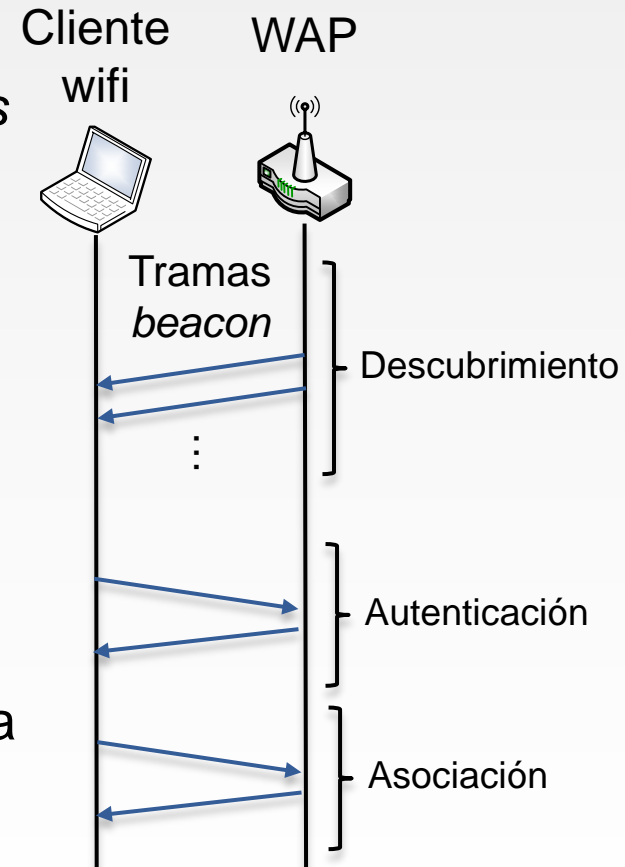
### Estándares IEEE 802.11

- IEEE 802.11, IEEE 802.11b, IEEE 802.11g y IEEE 802.11n disfrutaron de una aceptación internacional debido a que la banda de 2,4 GHz está disponible casi universalmente
- IEEE 802.11ac, conocido como Wifi 5, opera en la banda de 5 GHz
  - La banda de 5 GHz ha sido recientemente habilitada y por lo tanto existen menos interferencias
  - Su alcance es algo menor que el de los estándares que trabajan a 2,4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance)
- IEEE 802.11ah, conocido como Wifi HaLow proporciona conectividad inalámbrica en la Internet de las Cosas (*Internet of Things*, IoT)
  - Extiende su alcance hasta la banda de 900 MHz, adecuado para dispositivos de bajo consumo como sensores y dispositivos empotrados

## 3. Wifi

### Punto de acceso

- Un punto de acceso inalámbrico (*wireless access point*, WAP) es un dispositivo de red que permite la interconexión de equipos en una WLAN
- El área geográfica donde se puede obtener conectividad inalámbrica a través del WAP se suele denominar *hotspot*
- Normalmente proporciona conectividad con equipos de red cableados, típicamente usando tecnología Ethernet
- Los WAP tienen un rango de direcciones IPs para los dispositivos a los que proporciona servicio



## 3. Wifi

---

### Seguridad

- Por la propia naturaleza de las frecuencias de radio, las WLAN permite que un host no perteneciente a una red pueda intentar acceder a la misma sin autorización, y a menudo de forma fraudulenta
- Para solventar este problema, las WLAN implementan diferentes medidas de seguridad:
  - Autenticación para el ingreso en la red (SSID, *Service Set Identifier*)
  - Confidencialidad (cifrado) en las transmisiones



## 3. Wifi

---

### Seguridad

- La opción más común para garantizar la seguridad en redes wifi consiste en usar mecanismos de cifrado para el intercambio de datos
  - WEP (*Wired Equivalent Privacy*, Privacidad Equivalente a Cableado)
    - Utiliza criptografía de clave simétrica (claves de 64 o 128 bits) llamada PSK (*pre-shared key*)
  - WPA (*Wifi Protected Access*, Acceso Wifi protegido)
    - Utiliza criptografía de clave simétrica PSK de 128 bits
  - WPA2 (estándar 802.11i) es una mejora de WPA
    - En principio es el protocolo de seguridad más seguro para wifi actualmente

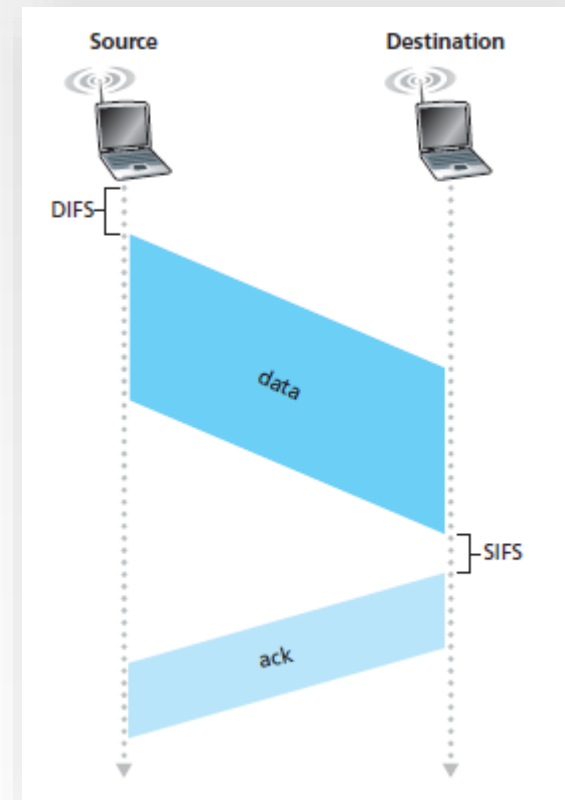
Tanto **WEP** como **WAP** son considerados **inseguros** actualmente

En octubre de 2017 se publicó un ataque llamado **KRACK** que permite descifrar las comunicaciones **WPA2**. Las diferentes plataformas (Android, Linux, etc) están publicando parches de seguridad que protegen los dispositivos frente a este ataque

## 3. Wifi

### Técnica de transmisión

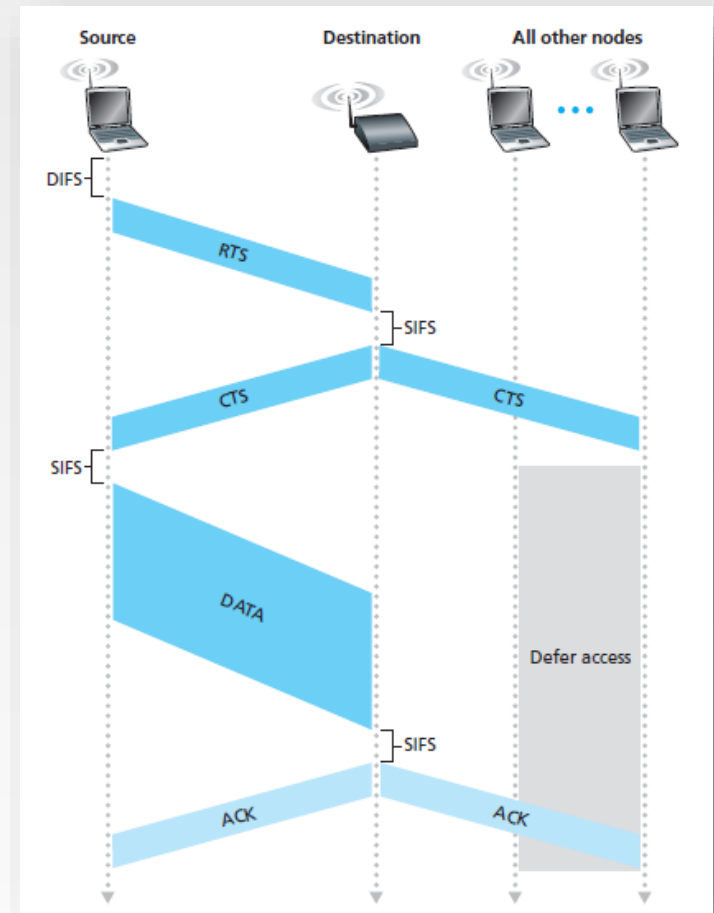
- Los estándares 802.11 usan un mecanismo llamado CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) acceso múltiple con escucha de portadora y evitación de colisiones para gestionar el acceso al medio:
  - Emisor:
    - Envía trama si el canal está vacío por un tiempo DIFS
  - Receptor
    - Envía ACK después de tiempo SIFS



## 3. Wifi

### Técnica de transmisión

- Reserva del medio en CSMA/CA
  - El equipo origen primero envía una trama corta de control de solicitud de transmisión RTS (*Request To Send*)
  - Si el equipo destino recibe esta trama significa que está preparado para recibir una trama. Este equipo devolverá una trama de contestación: preparado para transmitir CTS (*Clear To Send*) o receptor ocupado (RxBUSY).
  - Si la respuesta es afirmativa el equipo origen transmite la trama en espera (DATA)
  - Si el equipo destino recibe correctamente el mensaje contesta con la trama de confirmación positiva ACK (*Acknowledged*) y si no la recibe correctamente contesta con la trama de confirmación negativa NAK (*Not Acknowledged*)



## 3. Wifi

---

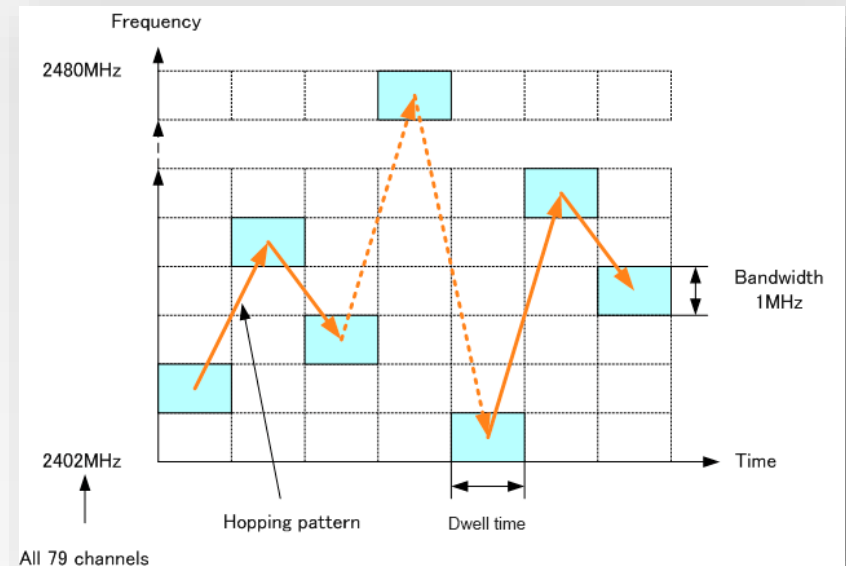
### Técnica de transmisión

- Los estándares IEEE 802.11 usan una técnica de transmisión por **espectro ensanchando**, que se basa en la transmisión de una señal con un ancho de banda mayor del ancho de banda del mensaje original. Esto tiene dos grandes ventajas:
  1. Menor potencia de emisión, al distribuir la energía a cada frecuencia. Esto provoca menos interferencia con otros receptores y que sea más difícil de detectar por intrusos (seguridad)
  2. Incorporación de redundancia, de manera que el mensaje está presente sobre diferentes frecuencias de las que se puede recuperar en caso de error
- Hay dos tipos:
  - Espectro ensanchado por salto de frecuencia (FHSS, *Frequency Hopping Spread Spectrum*)
  - Espectro ensanchado por secuencia directa (DSSS, *Direct Sequence Spread Spectrum*)

## 3. Wifi

### Técnica de transmisión

- El **salto en frecuencia (FHSS)** consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo
- Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia
- El orden en los saltos en frecuencia sigue una secuencia pseudoaleatoria acordada por el emisor y el receptor



Hedy Lamarr, 1942



## 3. Wifi

---

### Técnica de transmisión

- En la técnica de **secuencia directa (DSSS)** se genera un patrón de bits redundante (secuencia de Barker) para cada uno de los bits que componen la señal
  - Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0
  - El estándar IEEE 802.11 recomienda un tamaño de 11 bits (óptimo es 100)
- Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original
- La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que al resto de receptores les parecerá ruido menos al que va dirigida la señal

## 3. Wifi

---

### Otras tecnologías inalámbricas

- Bluetooth
  - Estándar IEEE 802.15
  - Especificación para Redes Inalámbricas de Área Personal (WPAN)
  - Enlace por radiofrecuencia en la banda de los 2,4 GHz
  - Alcance de 1 a 30 metros
- WiMAX: *Worldwide Interoperability for Microwave Access* (interoperabilidad mundial para acceso por microondas)
  - Estándar IEEE 802.16
  - Es una norma de transmisión de datos que utiliza las banda de 2,3 a 3,5 GHz
  - Puede tener una cobertura de hasta 50 km
  - Compite con el Wifi IEEE 802.11n

## 3. Wifi

---

### Otras tecnologías inalámbricas

#### ■ Redes móviles

- GSM (2G). Sistema global para las comunicaciones móviles (*Groupe Spécial Mobile*) es un sistema estándar de telefonía móvil digital
- GPRS (2.5G). *General Packet Radio Service*, extensión a GSM para la transmisión de datos. Velocidades de transferencia de bajada de 56-144 kbps
- UMTS (3G). *Universal Mobile Telecommunications System*, tecnologías móvil que proporciona velocidad de acceso a Internet elevada (velocidad máxima de 2 Mbit/s)
- LTE (4G). *Long Term Evolution*, evolución de UMTS (velocidades entre 100 Mbps y 1 Gbps)
- 5G. Tecnología sucesora del 4G, actualmente en desarrollo (su uso comercial está prevista para 2020)



## 3. Wifi

---

### Otras tecnologías inalámbricas

- Un dispositivo con conexión móvil puede ser utilizado como punto de acceso (WPA) para otros dispositivos
- Este proceso se conoce como **tethering**

