# Redes LAN Inalámbricas (Wi-Fi)


Prof. Mg. Daniel Lillo

# Definiciones

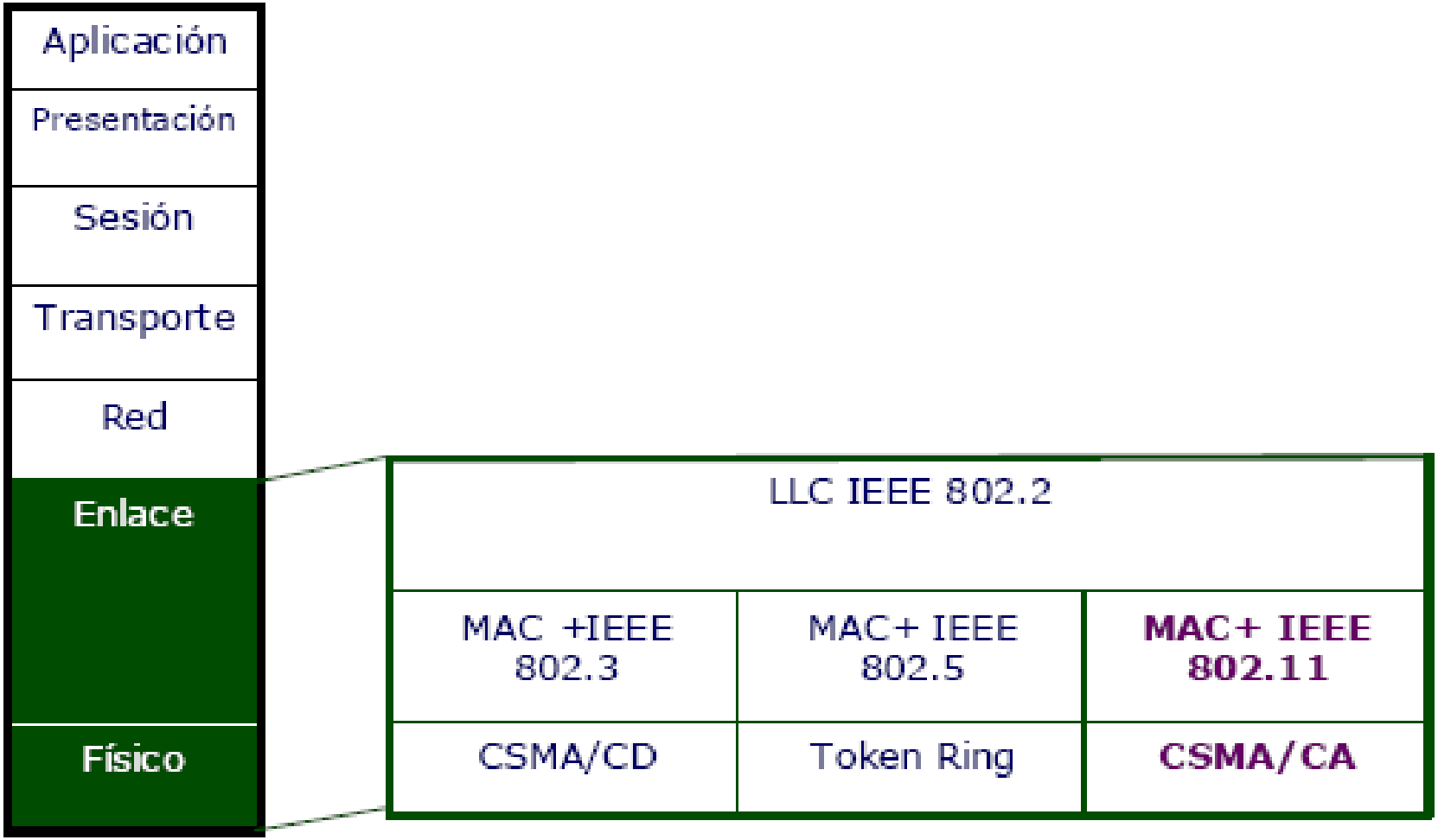
## ¿Qué es Wi-Fi?

- Es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11.
  - El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

## WLAN

- WLAN (Wireless Local Area Network) es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta.
  - Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.

# Arquitectura OSI



# WLAN

## Características Red WLAN

- **Movilidad:** este es un concepto importante en las redes 802.11, ya que lo que indica es la capacidad de cambiar la ubicación de los terminales.

- **Facilidad de instalación:** al no usar cables, se evitan obras para tirar cable por muros y techos, reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.
- **Flexibilidad:** puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso.

# Configuraciones WLAN (I)

- **Red de igual a igual**
  - Se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno.
  - Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Red peer-to-peer

# Configuraciones WLAN (II)

- **Cliente y punto de acceso**
  - Instalando un Punto de Acceso (APs) se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores.
  - Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata.
  - Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar.
    - Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso.

Cliente y punto de acceso

# Configuraciones WLAN (III)

- “Roaming”
  - Los puntos de acceso tienen un rango finito, del orden de 150m en lugares cerrados y 300m en zonas abiertas.
    - En zonas grandes es probablemente necesario más de un punto de acceso.
  - El objetivo es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso.
    - Esto es llamado "roaming“ (navegar).

Múltiples puntos de acceso y "roaming"

# Configuraciones WLAN (IV)

- **Redes con Puntos de Extensión**
  - Para resolver problemas particulares de topología, se puede usar un Punto de Extension (EPs) para aumentar el número de puntos de acceso a la red.
    - **Funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso.**
  - Los puntos de extensión extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión.
  - Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

Red con punto de extensión

# Estándares WiFi

| Estándares Wireless | | | |
|---|---|---|---|
| Estándar | 802.11b | 802.11a | 802.11g |
| Aprobado IEEE | Julio 1999 | Julio 1999 | Junio 2003 |
| Popularidad | Adoptado masivamente | Nueva tecnología, crecimiento bajo | Nueva tecnología con un rápido crecimiento |
| Velocidad | Hasta 11 Mbps | Hasa 54 Mbps | |
| Coste | Barato | Relativamente caro | Relativamente barato |
| Frecuencia | 2.4 - 2.497 Ghz | 5.15 - 5.35 Ghz<br>5.425 - 5.675 Ghz<br>5.725 - 5.875 Ghz | 2.4 - 2.497 Ghz |
| Cobertura | Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos | Cobertura baja, unos 150 metros, con mala conectividad con obstáculos | Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos |

# Estándares WiFi



| Estándares Wireless | | | |
|---|---|---|---|
| Estándar | 802.11b | 802.11a | 802.11g |
| Acceso Público | El número de Hotspots crece exponencialmente | Ninguno en este momento. | Compatible con los HotSpots actuales de 802.11b. El paso a 802.11g no es traumático para los usuarios |
| Compatibilidad | Compatible con 802.11g, no es compatible con 802.11a | Incompatible con 802.11b y con 802.11g | Compatible con 802.11b, no es compatible con 802.11a |
| Modos de datos | 1, 2, 5.5, 11 Mbps | 6, 9, 12, 18, 24, 36, 48, 54 Mbps | 1, 2, 5.5, 11 Mbps 6, 9, 12, 18, 24, 36, 40, 54 Mbps |
| Modulación | CCK | OFDM | OFDM y CCK |

# Estándares para redes inalámbricas (I)

| Estándar | Descripción |
|---|---|
| 802.11 | Estándar WLAN original. Soporta de 1 a 2 Mbps. |
| 802.11a | Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps. |
| 802.11b | Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps. |
| 802.11e | Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio. |
| 802.11f | Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores. |
| 802.11g | Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps. |
| 802.11h | Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico. |
| 802.11i | Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. |

# Estándares para redes inalámbricas (II)

- **IEEE 802.11**
  - La familia 802.11 actualmente incluye seis técnicas de **transmisión por modulación** que utilizan todas los mismos protocolos.
- **Normalización**
  - Los estándares IEEE 802.11b e IEEE 802.11g disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz que está disponible casi universalmente, con velocidades de hasta 11 Mbps y 54 Mbps, respectivamente.
    - Existe también el estándar IEEE 802.11n que está en desarrollo y trabaja a 2.4 GHz a una velocidad de 108 Mbps.
  - En los Estados Unidos y Japón, se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios.

# Estándares para redes inalámbricas (III)

- 802.11b
  - Ancho de banda máximo de hasta 11Mbps
  - Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
  - Las mismas interferencias que para 802.11
  - Conocido como WIFI
  - Modulación DSSS
  - Compatible con los equipos DSSS del estándar 802.11.
- 802.11g
  - Ancho de banda máximo de hasta 54 Mbps
  - Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
  - Compatible con 802.11b.
  - Modulación DSSS y OFDM.
- 802.11a
  - Ancho de banda máximo de hasta 54 Mbps
  - Opera en el espectro de 5 Ghz sin necesidad de licencia. Menos saturado
  - No es compatible con 802.11b y 802.11g
  - Modulación de OFDM.

# Capa Física (I)

- El estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de LAN inalámbricas. Este estándar no sólo engloba la tecnología de radiofrecuencia sino también la de infrarrojos. Asimismo, incluye varias técnicas de transmisión como:
  - Modulación por saltos de frecuencia (FHSS)
  - Espectro de extensión de secuencia directa (DSSS)
  - Infrarrojos (IR)
  - Multiplexación por división en frecuencias octogonales (OFDM)

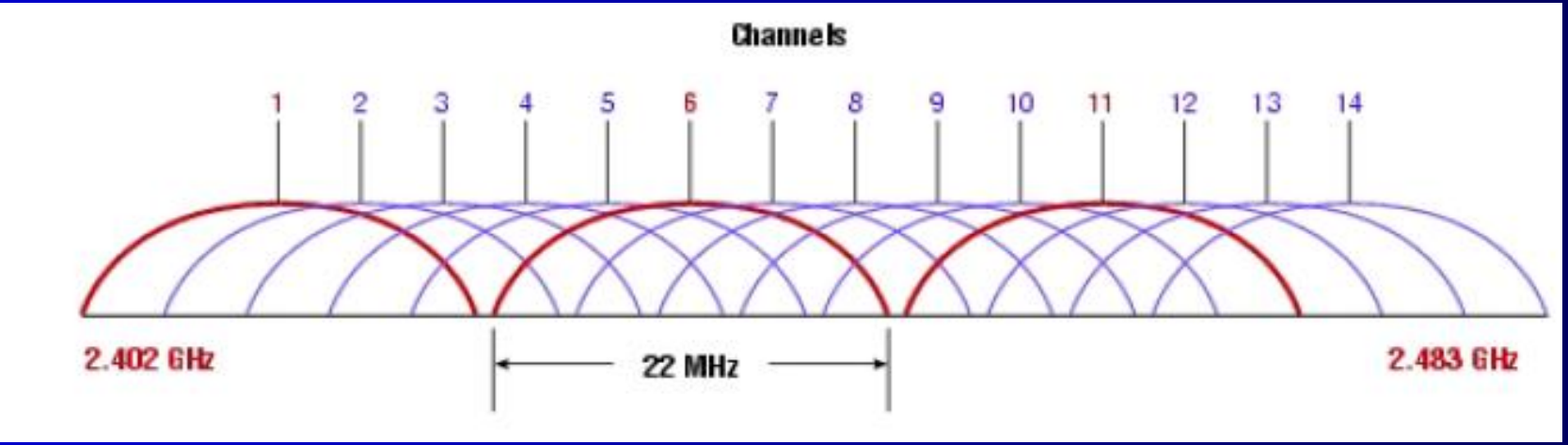
| Norma | Banda de frecuencia | Modulación | Alcance | Velocidad máxima | Nº máx. canales sin solap. |
|---|---|---|---|---|---|
| 802.11 b | 2.4 GHz | DSSS | 100 m | 11 Mbps | 3 |
| 802.11 a | 5 GHz | OFDM | 50 m | 54 Mbps | 12 |
| 802.11 g | 2.4 GHz | OFDM | 100 m | 54 Mbps | 3 |

# Capa Física (II)

- **IEEE 802.11 divide el espectro en canales disponibles de 22 MHz. Los canales están superpuestos.**
- **Frecuencias:**
  - 2412–2462 MHz (Norte América)
  - 2412–2472 MHz (Europa estándar)
  - 2412 – 2484 MHZ (Japón)
- **Canales:**
  - 1–11 canales (Norte América)
  - 1–13 canales (Europa stándar)
  - 1 – 14 canales (Japón)

**No todos los canales están disponibles en todos los países**

- **Por ejemplo de estos 13 canales disponibles en Europa los canales 1, 6 y 11 son los que presentan entre sí baja interferencia y/o superposición. (Usados en las tecnologías 802.11b, 802.11g)**



# Capa De Enlace (I)

- **Protocolo CSMA/CA**
  - Es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos.
  - Es un método de acceso de red en el cual cada dispositivo señala su intento para transmitir antes de que lo haga realmente.
    - Esto evita que otros dispositivos envíen la información, así evitando que las colisiones ocurran entre las señales a partir de dos o más dispositivos.
  - En CSMA/CA, tan pronto como un nodo recibe un paquete que deba ser enviado, comprueba que el canal esta libre. Si el medio o canal esta libre , entonces el paquete es enviado después de esperar por un corto periodo de tiempo; pero si el canal esta ocupado, el nodo esperara por un periodo de backoff.

# Capa de Enlace II

**Formato de las tramas MAC**

**Las tramas MAC contienen los siguientes componentes básicos:**

- una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia
- un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama
- un secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits

**Las tramas MAC se pueden clasificar según tres tipos:**

- Tramas de datos.
- Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda
- Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

# Capa De Enlace (III)

## Formato de trama MAC

- Estas tramas poseen tres componentes: MAC Header, Body y Frame Check Sequence (FCS).

| Octetos: | 2 | 2 | 6 | 6 | 6 | 2 | 6 | 0-2312 | 4 |
|---|---|---|---|---|---|---|---|---|---|
| | Frame Control | Duration / ID | Address 1 | Address 2 | Address 3 | Sequence control | Address 4 | Body | FCS |
| | *MAC Header* | | | | | | | *Body* | *FCS* |

- Campo de control. Merece examinar aparte. Lo haremos más abajo.

- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.

- Campos address1-4. Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

- Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.

- Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.

- FCS. Contiene el checksum.

# Capa De Enlace (IV)

## MAC Header- Frame Control

Si se analiza en detalle los dos octetos del campo control, los mismos están compuestos por los siguientes subcampos

| Bits: | 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Protocol Version | Type | Subtype | To DS | From DS | More Frag | Retry | Pwr Mgt | More data | WEP | Order |

- Versión.

- Type/Subtype. Mientras tipo identifica si la trama es del tipo de **datos, control o gestión**, el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.

- ToDS/FromDS. Identifica si la trama si envía o se recibe al/del **S**istema de **D**istribución. En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS.

- Más fragmentos. Se activa si se usa fragmentación.

- Retry. Se activa si la trama es una retransmisión.

- Power Management. Se activa si la estación utiliza el modo de economía de potencia.

- More Data. Se activa si la estación tiene tramas pendientes en un punto de acceso.

- WEP. Se activa si se usa el mecanismo de autenticación y encriptado.

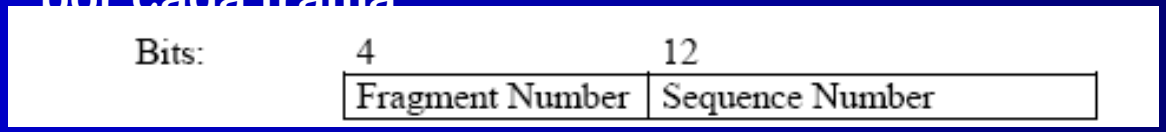
- Order. Se utiliza con el servicio de ordenamiento estricto.

# Capa De Enlace (V)

- Duration ID, el cual consta también de 2 octetos.
  - En la mayoría de los casos indica la duración de la trama, cuyo valor oscila entre 0 y 32767.

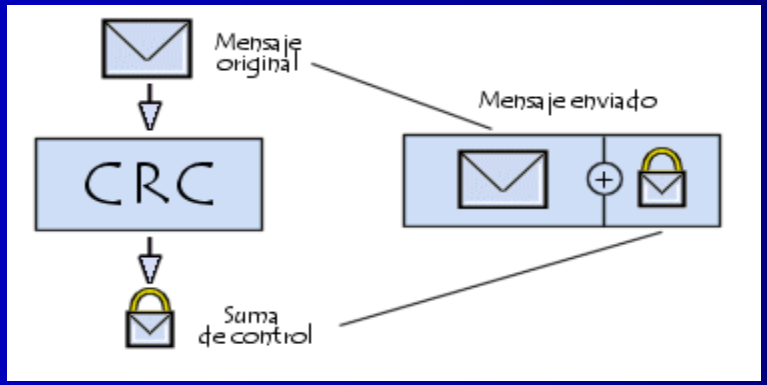
- Los otros campos que incluye la trama son los de direcciones, los cuales son empleados para indicar el BSSID.
    - BSSID es la dirección MAC de un adaptador inalámbrico o un Punto de Acceso.

- El campo que queda es el de Sequence Control Field que tiene 16 bits y consiste en 2 subcampos:
  - Fragment Number: (4 bits) Si se emplea fragmentación, este campo indica cada uno de los fragmentos, caso contrario es cero.
  - Sequence Number: (12 bits) es un valor que se asigna a cada MSDU generada y oscila entre 0 y 4096, incrementándose en 1 por cada trama



# Capa De Enlace (VI)

- Body
  - En el campo del cuerpo de la trama se encuentran los datos de la transmisión.
- FCS
  - La cola de una trama 802.11 es el FCS (Frame Control Sequence) que es el CRC de grado 32, que corresponde al estándar IEEE CRC-32.




$$G_{(x)} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

## Capa LLC

- Es el protocolo que se sitúa sobre la capa MAC.
- Se encarga del control del enlace lógico

# Compatibilidad de dispositivos inalámbricos

- Los sistemas inalámbricos de redes LAN de distintos vendedores pueden no ser compatibles para operar juntos. Tres razones:
  - Diferentes tecnologías no interoperarán.
    - Un sistema basado en la tecnología de Frecuencia esperada (FHSS), no comunicará con otro basado en la tecnología de Secuencia directa (DSSS).
  - Sistemas que utilizan distinta banda de frecuencias no podrán comunicar aunque utilicen la misma tecnología.
  - Aún utilizando igual tecnología y banda de frecuencias ambos vendedores, los sistemas de cada uno no comunicarán debido a diferencias de implementación de cada fabricante.

# Seguridad en redes WIFI (I)

- **Medidas básicas:**
  - Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio, es la encriptación.
  - Encriptación
    - **La encriptación significa que los datos son cifrados antes de que se envíen a través de la red inalámbrica y se reagrupan cuando se obtienen por el destinatario, haciéndoles así ilegibles para otros usuarios de la red.**
    - **En general se utiliza WEP (Wired Equivalent Privacy), que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso.**
      - **La clave de acceso estándar es de 40 bits, pero existe otra opcional de 128 bits, y se asigna de forma estática o manual, tanto para los clientes, que comparten todos el mismo conjunto de cuatro claves predeterminadas, como para los puntos de acceso a la red, lo que genera algunas dudas sobre su eficacia.**
      - **WEP utiliza un esquema de cifrado simétrico en el que la misma clave y algoritmo se utilizan tanto para el cifrado de los datos como para su descifrado**

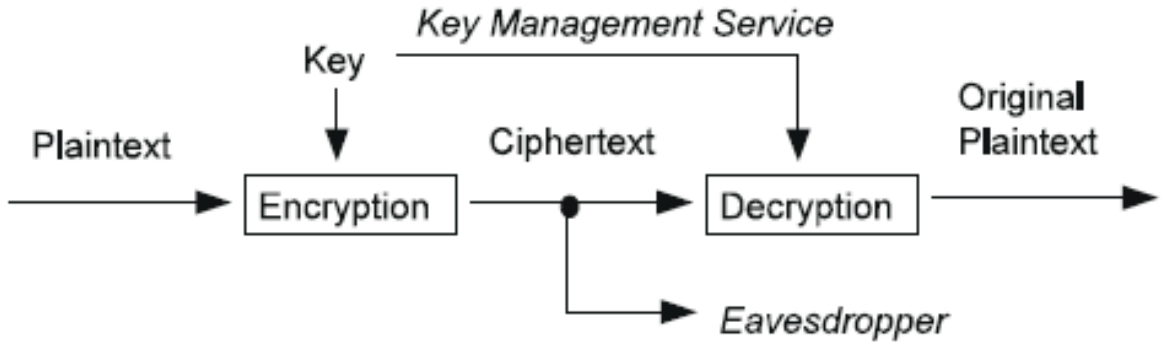
# Seguridad en redes WIFI (II)

- La funcion de encripcion *E* opera sobre *P* para producir *C:*

  $E\,k\,(P) = C$

- En el proceso inverso, la funcion de desencripcion *D* opera sobre *C* para producir *P:*

  $D\,k\,(C) = P$



# Seguridad en redes WIFI (III)

- Filtrado de direcciones MAC
  - La habilitación del filtrado de direcciones MAC permite la inclusión o exclusión de usuarios sobre la base de sus direcciones MAC, que son únicas. Los usuarios no presentes en la lista serán rechazados o se les concederá acceso limitado a la red.
- SSID
  - El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.
  - Es como un gestor de asignación de nombres, que proporciona un control de acceso muy rudimentario, razón por la que apenas se utiliza en las implementaciones comerciales.
- Cambio periódico de las claves de encriptación
  - Cambiar las claves de encriptación, periódicamente, impide que usuarios no autorizados accedan a la red inalámbrica, después de haber recuperado la clave una vez.

# Seguridad en redes WIFI (IV)

- **Implementación de una mayor seguridad :**
  - Las características de seguridad anteriormente descritas, están disponibles para cualquier dispositivo inalámbrico que cumpla los estándares.
  - Para las organizaciones que requieran mayor seguridad, existen medidas de seguridad adicionales que pueden integrarse en la configuración de los dispositivos inalámbricos.
    - Tecnologías tales como **VPN**, autentificación **RADIUS** y **802.1x** proporcionan mejores medios de protección contra el acceso mal intencionado a la red.