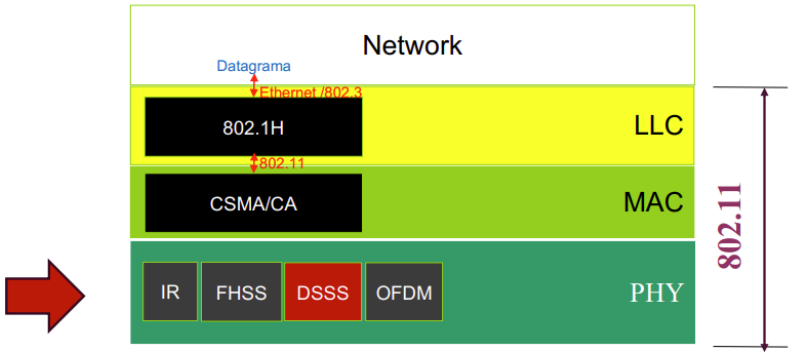
TEMA 4. DCLAN

WIFI

- **Tecnologías WPAN.** Ofrecen conectividad inalámbrica a dispositivos de un único usuario. Distancia de unos pocos metros. Algunas son ***RFID, Bluetooth o ZigBee.***
- **Tecnologías WLAN.** Basada en WiFi (*estándar IEEE 802.11*). En crecimiento, y adoptada en todo el mundo. Distancia de 100m a 10km.
  - **WiMax:** Basada en *IEEE 802.16*, era una alternativa a ADSL para zonas rurales. Bandas de frecuencia de 2 a 11 GHz. Hasta 70 Mbps a una distancia de 50km. No tuvo éxito.

ESTÁNDAR IEEE 802.11



IR: Infrared light
FHSS: Frequency hopping Spread spectrum
DSSS: Direct sequence Spread spectrum (802.11b) (11Mbps)
OFDM: Orthogonal frequency-division multiplexing

CSMA/CA: Carrier Sense Multiple Access with Collission Avoidance

802.1H: Bridge Tunnel Service → tráfico a través de una red 802.3 (Ethernet)

Evolución de los estándares.

- El primero con éxito comercial fue **802.11b** *con 2.4 GHz* ***y 11 Mbps.***
- **802.11a** *(5.0 GHz)* **y 802.11g** *(2.4GHz)* alcanzan una transmisión máxima de ***54 Mbps.***
- **802.11n** ocupa una banda *2.4/5.0 GHz* ***a 600 Mbps.***
- **802.11ac** (versión 1) **y 802.11ac** (versión 2) ocupan ambos a *5.0 GHz* con una transmisión de ***1.73 Gbps y 3.46 Gbps*** respectivamente.
- El más reciente es **802.11ax** con *2.4/5.0/6.0 GHz* alcanzando ***9.60 Gbps.***

PHY: IR

¿Con el mando de la tele podemos apagar la del vecino? No.

El infrarrojo tiene propiedades similares a la luz visible (no puede atravesar obstáculos físicos como paredes, esto es bueno para la seguridad).

- **VENTAJA:** Gran ancho de banda.
- **DESVENTAJA:** Sensible a radiaciones.

Quedó descartado para redes WiFi.

Surge la idea de **LiFi**: comunicaciones basadas en la luz de las bombillas del techo, que emiten no solo luz sino también información.

PHY: Spread Spectrum

La idea es transmitir información en un ancho de banda mayor para evitar interferencias, mejorar la inmunidad y dificultar su interceptación. Operan en bandas que NO necesitan licencia.

- **Espectro expandido con salto en frecuencia (FHSS):** Inventado por Hedy Lamarr. La señal salta entre diferentes frecuencias siguiendo una secuencia de saltos (se sigue usando en bluetooth).
- **Espectro expandido con secuencia directa (DSSS):** se consigue inmunidad al ruido utilizando un canal de 22 MHz del que en realidad solo utilizamos los dos 2 MHz centrales. Utilizada en *802.11b.*

Se envía una secuencia de 11 bits (**Barker Code o PRN**): si el primer bit es 0 se manda tal cual, y si es 1 se manda la secuencia invertida. Al compararlas pueden no coincidir hasta 5 bits.

Bandas sin licencia.

El WiFi usa **bandas sin licencia**, lo que significa que cualquiera puede transmitir respetando las restricciones de la banda. Las bandas de frecuencias destinadas a comunicaciones de radio (WiFi, Bluetooth, WirelessUSB, Zigbee) son la de **2.4 GHz** y la de **5 GHz**.

En EE.UU:

Industrial, Scientific, and Medical **(ISM).**

- Banda 900 MHz. Actualmente no utilizado por WLANs
- Banda 2.4 GHz.

Unlicensed National Information Infrastructure **(UNII):**

- 4 bandas entre 5.15 GHz – 5.835 GHz.

En Europa:

Bandas aprobadas por el CEPT (European Conference of Postal and Telecommunications Administrations):

- Banda 2.4 GHz, basado en **ISM.**
- 3 bandas entre 5.15 GHz – 5.875 GHz.

Velocidad de transmisión adaptativa.

La velocidad se adapta a la potencia con la que nos llega la señal (por eso al alejarnos de una red WiFi notamos que la conexión funciona 'mal').

Señal microondas.

Banda de frecuencia sobre la que opera WiFi, que se ve afectada por:

- **Absorción:** El H2O y el metal absorben las ondas WiFi y dificultan su propagación.
- **Reflexión:** una señal electromagnética choca sobre una superficie y rebota. En el caso de WiFi es una reflexión controlada que se aprovecha para dirigir las ondas.
- **Interferencia:** si dos señales están en la misma fase que interfieran, aumentaría su potencia (interferencia constructiva). Si la fase es distinta, disminuye (interferencia destructiva).
- **Difracción:** si hay un obstáculo entre dos antenas, la onda se dispersa y cubre mayor distancia, pero con menor potencia.

Línea visual (LOS, Line of Sight): cuando transmitimos entre dos estaciones, la zona sin obstrucciones (**Zona de Fresnel**) no tiene que ser una línea, sino un radio que aumenta cuanto mayor es la distancia a la que se quiere transmitir.

Calidad de la señal.

$$\mathrm{dBm} = 10 \times \log \frac{P}{1\mathrm{mW}}$$

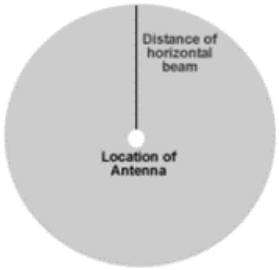
```
  1 mW = 0 dBm
  2 mW = 3 dBm
100 mW = 20 dBm
  1 W  = 30 dBm
```

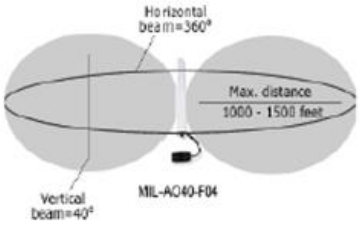
Rango óptimo para WiFi entre -40 y -90 dBm

Antenas.

Patrón de radiación: la radiación se mide mediante dBi haciendo uso del modelo teórico de una antena puntual (irradiaría en todas las direcciones con igual potencia).

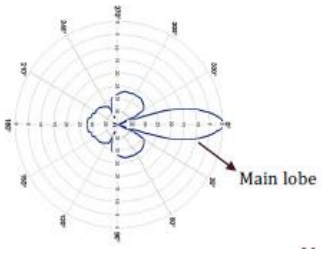
- Antenas omnidireccionales: desde un plano horizontal la potencia sería común en todas las direcciones. Dese un plano vertical no.





Mientras mayor ganancia de dBi, menor ángulo del haz vertical y mayor distancia.

- Antenas direccionales: No hay ningún plano en el que la potencia sea similar en todas las direcciones. La forma se asemeja a la de una bombilla.
    - Tipo panel:
        - Ganancia: 3-15 dBi
        - Haz vert./horiz. 30-60º
        - Dist. Máxima: 4 km
    - Yagi:
        - Ganancia: 18 dBi
        - Haz vert./horiz. 15º
        - Dist. Máxima: 6 km
    - Parabólica:
        - Ganancia: 19-28 dBi
        - Haz vert./horiz. 6-16º
        - Dist. Máxima > 6km



IEEE 802.11 – CONCEPTOS BÁSICOS

Estación: un PC, un móvil, etc. No hace de sistema de distribución (no distribuye tramas como lo haría un punto de acceso). El controlador de la tarjeta modifica la trama WiFi para que se convierta en una tarjeta Ethernet.

Punto de acceso (AP): Puente entre el entorno inalámbrico y entorno cableado. Ofrece un sistema de distribución a las estaciones asociadas a él. Soportan *roaming*, funciones de sincronización (*beaconing),* soporte para gestión de energía. El tráfico fluye siempre a través del punto de acceso.

Funcionamiento IEEE 802.11.

Mediante **Basic Service Set (BSS)**. Las estaciones que están dentro pueden hablar entre ellas mediante un AP. El diámetro de una célula es el doble de la distancia máxima entre dos estaciones.

IBSS (Independent Basic Service Set). Si no hay AP (*ad-hoc*) para las comunicaciones. Una estación inicia la red y la coordina. Aunque hay una distancia máxima entre dos estaciones, se puede extender la red conectando con terceras estaciones, formando una **MANET**.

ESS (Extended Service Set). Varios BSS se unen mediante un **DS (Distribution System).** La red que forman se identifica mediante el **SSID (nombre de la red)**. Aunque el diámetro es igual al de un BSS, no existen restricciones para el radio de cobertura de la red general.

El **DS** se encarga de entregar los paquetes al AP adecuado. Puede ser integrado (solo un AP conectado a una red cableada), cableado (varios APs conectados a una red cableada) o inalámbrico (WDS, APs comunicados vía inalámbrica).

El **BSSID** es el MAC del AP de cada BSS (será por tanto distinto en cada célula). Si no hay AP (IBSS) es un valor aleatorio.

IEEE 802.11 – CSMA/CA

MAC 802.11: Sus principales funcionalidades son:

- **Controlar el acceso al medio:** dos servicios de tráfico (DFC [servicio de datos asíncrono] obligatorio y PCF [servicio con restricción temporal] opcional) y tres métodos de acceso (CSMA/CA que es obligatorio y RTS/CTS o PCF, que son opcionales).
- **Entrega fiable de datos:** mediante intercambio de ACKs, solucionar problema de nodos ocultos y operar correctamente en medios con ruido. Para tramas de gran tamaño se utiliza **RTS/CTS**.
- **Protección de datos.**

CSMA/CA.

Si el canal permanece libre durante un período igual a *DIFS*, la estación puede transmitir de forma inmediata.

Si el medio está ocupado, la estación tiene que esperar un tiempo igual a *DIFS* + tiempo aleatorio de *back-off*. Si otra estación ocupa el medio, el temporizador para.

El receptor responde tras un tiempo SIFS con un ACK si el paquete se ha recibido sin errores.

Inter-frame spacing	
SIFS	Período más corto. Para mensajes ACK, CTS, etc. **Prioridad alta.**
PIFS	Para servicio con restricciones temporales de PCF. **Prioridad media**
DIFS	Para servicios asíncronos de datos. **Prioridad baja.**
EIFS	Utilizado cuando hay errores de transmisión. **No es un tiempo fijo.**

Retransmisiones: suceden cuando una transmisión falla (el emisor no recibe el ACK). Las tramas broadcast (difusión) no permiten retransmisión por no haber una estación de destino explícita.

El número de retransmisiones está limitado por el tamaño de paquete y el umbral RTS:

Contador de reintentos	Tamaño trama	Máx. intentos
SLRC station long retry counter	>= umbral RTS	7
SSRC station short retry counter	< umbral RTS	4

Las tramas de *broadcast/multicast* utilizan difusión por lo que sólo hay un intento de retransmisión.

Collision avoidance.

Si pasado un tiempo DIFS el canal no está libre, entra en este modo. Hay que esperar un tiempo *DIFS* + *backoff* antes de que el canal esté libre para transmitir. El **backoff con DCF** se hace del siguiente modo:

- Cuando se transmite un paquete por primera vez: intervalo de backoff [0, cw], donde cw es la ventana de contención, inicialmente igual a **15 * cw_{min}.**
- Cuenta atrás desde el valor elegido cuando el medio esté libre. Si durante la cuenta atrás se ocupa el medio, ésta se pausa. Si llega a 0, transmitir.
- Si hay que retransmitir la trama: se duplica el tamaño de cw hasta cw_{max} = 1024.

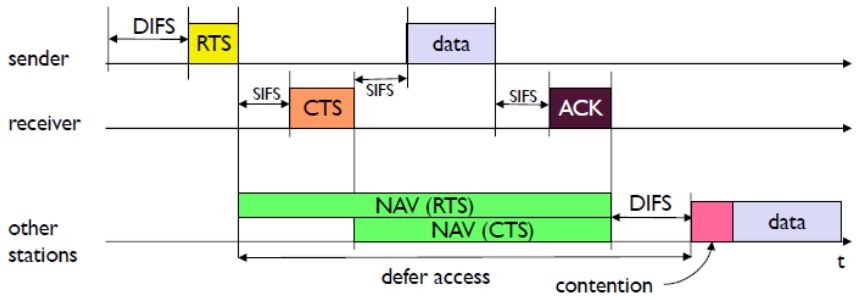
Mecanismo RTS/CTS.

Permite solucionar el **problema del nodo oculto**. Tenemos dos terminales A y C conectados a un punto de acceso B. B puede ver ambos terminales, pero entre ellos no se alcanzan a ver. Al no conocer de la existencia de otro, podría transmitir a la vez, lo que provocaría una colisión.

Para solucionarlo, cuando A quiera mandar datos a B, le mandará un RTS a todas las estaciones que estén en su rango de alcance (incluida B).

El punto de acceso B responderá con un CTS a todas las estaciones que estén en su alcance (no solo A, sino también a C). Al recibirlo, el resto de las estaciones no mandarán nada.

Los paquetes RTS/CTS establecen la duración esperada de la comunicación entre A y B (transmisión + ACK).



Point coordination function (PCF): Requiere de DCF para funcionar. Durante un **CFP (Contention Free Period)**, un AP genera un *beacon* con la lista de estaciones conectadas que soportan PCF y les manda un *point*, un mensaje con el que les pregunta si tienen algo que transmitir.

Este periodo finaliza con un CF_{end}. El CFP se alterna con el **CP (Contention Period)**, durante el cual las transferencias se hacen según las reglas del DCF.

IEEE 802.11 – MANAGEMENT

A partir de la MIB obtenemos información de estado. Tenemos:

- **MAC MIB** a nivel MAC.
- **PHY MIB** a nivel físico.

Proceso de conexión.

1. **Scanning:** Es el proceso de identificar las redes inalámbricas en la zona. Hay dos tipos:

   Pasivo. El cliente debe esperar a recibir los *beacons* de los diferentes AP.

   Activo. El propio cliente manda un *probe request* a los APs y estos le responden con un *probe response*.

Esta fase da como resultado una lista de todas las BSSs descubiertas y sus parámetros (BSSID, SSID, intervalo de beacon, etc.). El usuario escoge la red que desee (**Joining**).

2. Autenticación: Existen dos métodos, *open-system* donde todo el mundo se autentica y autenticación por *shared-key*.

Pre-autenticación: se da cuando en una misma red nos desconectamos de un AP y nos conectamos a otro destino. En vez de esperar a perder totalmente la conexión, cuando se detecta pérdida de señal del primer AP y buena señal con el segundo, se inicia el proceso de autenticación con este último.

3. Asociación: El AP registra la MAC del cliente. La estación *(por ejemplo, el móvil del cliente*) manda un mensaje AP *register* ($IP_{station}$, $MAC_{station}$) para que el AP lo propague por toda la red para reconfigurar los switches y APs del resto de la red.

Re-asociación: Si pasamos de un AP a un AP nuevo, los APs pueden establecer una comunicación entre ellos para que el antiguo pueda pasarle al nuevo las tramas pendientes de envío.

Conservación de la energía: APs siempre activos, retrasan la transmisión de tramas de STA (estación del cliente). No recomendable.

Sincronización con *beacons*: "como curiosidad, no hay que saberlo de memoria", los APs configuran su reloj interno con los STAs mediante los *beacons* y su TSF (*Time synchronization function*).

IEEE 802.11 – FORMATO DE TRAMAS

Preámbulo:

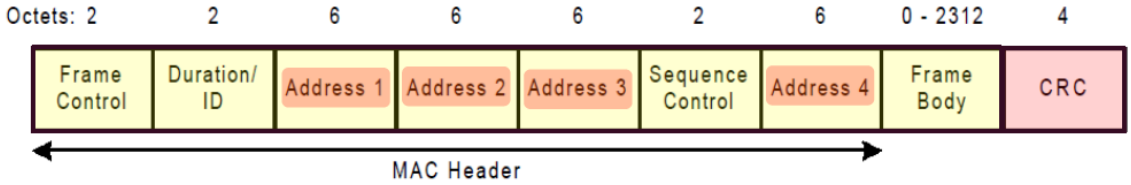
SYNC	(80 bits) (010101…)
SFD	(Start Frame Delimiter) (16 bit) (0000.1100.1011.1101)

PLCP Header:

PLCP=PHY Layer Convergence Protocol (**Tx a 1Mbps**)

PLCP_PDU Length Word	Número de bytes en la trama
PLCP Signaling Field	Velocidad de Tx
Header Error Check Field	16 bits CRC

MAC Data:



Observar que tanto el PLCP Header como MAC Data tienen un CRC. La trama mide como mínimo 0 bytes y como máximo 2312 bytes.

El tamaño depende del tipo de trama que enviemos (hay varios tipos: control, datos o gestión). Viene definido por **frame control**.

Sequence control establece a partir de qué tamaño se fragmetan las tramas. Cada trama lleva un identificador que numera la trama en la secuencia de envío.

Cuatro campos de direcciones: cuando la trama va destinada al AP el bit "To DS" vale 1. Cuando parte del AP es el bit "From DS" el que vale 1.

To DS	From DS	Address 1	Address 2	Address 3	Address 4	
0	0	DA	SA	BSSID	N/A	← AdHoc
0	1	DA	BSSID	SA	N/A	Infraestructura
1	0	BSSID	SA	DA	N/A	Infraestructura
1	1	RA	TA	DA	SA	← WDS

DA : Destination Add. Destino final
SA : Source Add. Origen
RA : Recipient Add. Siguiente destino
TA : Transmitter Add. Anterior transmisor
BSSID : Infraestructura → AP MAC Address
AdHoc → valor aleatorio

Si “To DS” = 0 y “From DS” = 0: estamos en una red *adHoc* (no hay AP).

El BSSID también funciona como dirección: es el identificador de la red, pero también la dirección MAC del AP (salvo en la red *adHoc*, donde es un valor aleatorio).

Address 1: Dirección del dispositivo que recibe la trama.

Address 2: Dirección del dispositivo que envía la trama.

Address 3: BSSID si estamos en adHoc. Si no, depende de qué dirección de las dos anteriores sea la del PA.

Si es la Address 1: dirección de destino final de la trama.

Si es la Address 2: dirección de origen de la trama.

Address 4: Dirección de origen de la trama. Solo se ocupa cuando las otras tres direcciones tienen un valor asociado y ninguno es el de dirección de origen de la trama.

Topologías de red.

IBSS o red Ad Hoc: Ningún elemento de la red es imprescindible. Los nodos operan como routers. La seguridad es por clave compartida.

Extended basic service set (ESS): Varios APs formando una única red. Comparten un mismo SSID y se comunican entre sí mediante switches Ethernet.

WDS: Requiere que los APs estén operando en un mismo canal, tienen que usar el mismo tipo y clave de cifrado y cada conexión WDS debe ser definida explícitamente en cada AP. Un AP puede actuar como:

Simple: acepta clientes, pero no se conecta a otros AP.

Puente (bridge): Los bridges permiten conectar dos edificios cuando no es posible conectarlos por cable. Se puede conseguir cubrir grandes distancias (unos pocos kilómetros) utilizando antenas direccionales.

Repetidor: Un punto de acceso sin conexión a la red cableada permite extender la cobertura del AP original sin necesidad de gastos importantes en infraestructura.

Prestaciones WDS con 802.11b.

A continuación, se presentan varios casos en los que tenemos dos portátiles, cada uno conectado a un AP. Se mide el *throughput* por envío de tramas de un portátil a otro.

Escenario 1 (mejor caso): Cada portátil está conectado por cable a su AP. Los APs están conectados al canal 1 (en este canal suceden las únicas pérdidas que pueda haber).

Escenario 2: El AP izquierdo es un repetidor. Está conectado a su portátil mediante un enlace inalámbrico, lo que provocará dos transmisiones por trama y una bajada del *throughput*.

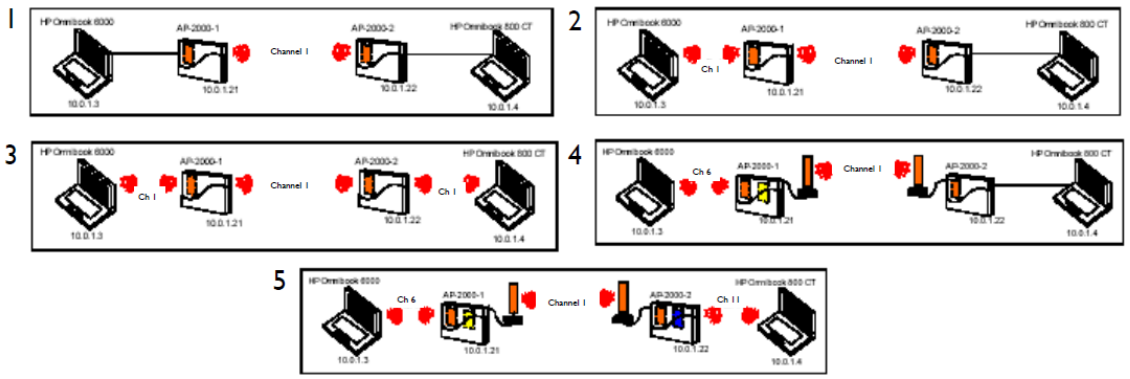
Escenario 3 (peor caso): Ambos AP están funcionando como repetidores. La capacidad del canal cae a un tercio (tres transmisiones por trama).

Para alcanzar mayor rendimiento se puede utilizar más de un canal por cada AP.

Escenario 4: El AP izquierdo se conecta por un canal al portátil y por otro al otro AP. El AP derecho se conecta por cable a su portátil. Hay pérdidas en ambos canales, pero al no haber dos APs en el mismo, no hay competición por su uso.

Escenario 5: Los dos APs se conectan a su portátil por enlace inalámbrico. Ambos usan canales diferentes. Es algo peor que el escenario 4 (por dos enlaces inalámbricos) pero mejor que el 3.

Escenario	Maximum Throughput	Average Throughput
1	4,59 Mbit/s	3,46 Mbit/s
2	2,22 Mbit/s	1,90 Mbit/s
3	1,87 Mbit/s	1,61 Mbit/s
4	3,64 Mbit/s	2,79 Mbit/s
5	3,19 Mbit/s	2,28 Mbit/s



Topología avanzada: mallas. Varios APs enlazadas en un mismo canal que provocan mayor interferencia. Comparten además la misma clave, lo cual imposibilita que este modelo sea apto para seguridad empresarial.

Configuración en estrella: Se sitúan en la zona wireless todos los APs y todos están a un hop (salto) de distancia del AP central (el que está conectado con la red cableada).

Configuración en cadena: Los APs están conectados en cadena, lo que implica que una vez entramos en la zona wireless podríamos tener que dar varios hops desde el AP central para llegar hasta el que queremos.

Esta topología plantea problemas de latencia, pérdidas, competiciones entre los APs por ver quién ocupa el enlace, wireless más lento... es el peor caso.

Configuración en anillo: Tras activar el protocolo STP en todos los APs, tenemos las mismas ventajas que en ethernet: si un AP falla, se puede reemplazar por otro.

En resumen, a nivel de **ventajas** de WDS tenemos un menor coste y mayor flexibilidad. Entre sus **desventajas** se encuentra la pérdida de prestaciones o cifrado únicamente por WEP o WPA/WPA2 con clave compartida.

802.11 – SEGURIDAD

Los pilares de la seguridad son la **autenticación** (solo usuarios autorizados acceden al sistema), la **integridad** (evitar modificación de datos) y la **confidencialidad** (evitar capturas de datos por terceros).

Tres generaciones de cifrado: WEP, WPA y WPA-2.

¿Cómo cambia WEP el establecimiento de la conexión? En la fase de autenticación se hará uso de una WEP Shared Key y tras la fase de asociación la comunicación se encriptará mediante WEP.

> Autenticación open-system: (1) El cliente intenta autenticarse y (2) el AP para determinar qué clientes se pueden conectar a la red filtra por dirección MAC. El problema de este sistema es que la dirección MAC se puede modificar.
>
> Autenticacón por shared-key: (1) El cliente intenta autenticarse, (2) el AP le responde con un *challenge text* que (3) el cliente cifra con su clave y le reenvia al AP. (4) El AP comprueba si está cifrado correctamente y si no es así, rechaza al cliente.

Criptografía – conceptos básicos.

El protoclo WEP utiliza para cifrado **RC4**. Se basa en una clave secreta compartida (shared-key) por las estaciones y el AP de la red.

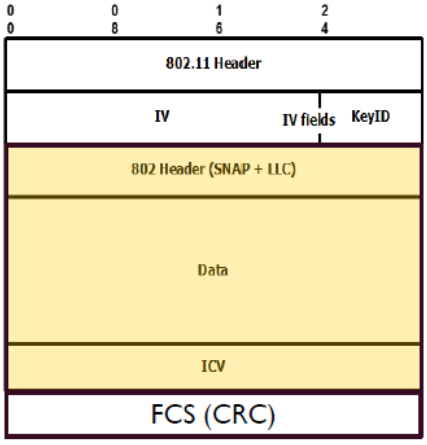
Para cifrar los datos se hace *datos XOR keystream* (secuencia pseudoaleatoria que conoce tanto la fuente con el AP generada a partir de la shared-key). Para descifrarlos habría que hacer el mismo XOR (simetría).

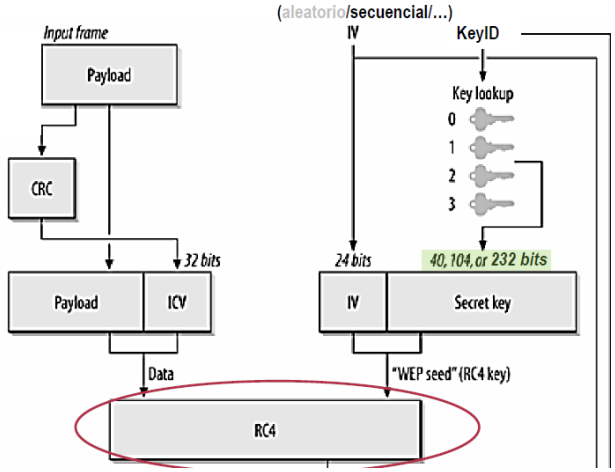
Ataque por fuerza bruta: Si el atacante consigue el texto cifrado y conoce algunas partes del texto en claro puede averiguar cuál es el valor del *keystream* en esas partes y a partir de esto obtener la shared-key que lo generó.

Sabiendo que una clave de 8 caracteres permite 100^8 combinaciones de keystreams distintas y que cada keystream ocupa 2 KB podemos calcular la ocupación en memoria de todas las keystreams que una key puede generar como 100^8 * 2 KB = 2 Tbytes.

El error catastrófico de WEP es que el AP manda un texto en claro que el cliente debe cifrar. El atacante puede obtener tanto el texto cifrado como el texto sin cifrar, obteniendo fácilmente la clave.

Cifrado WEP al detalle.

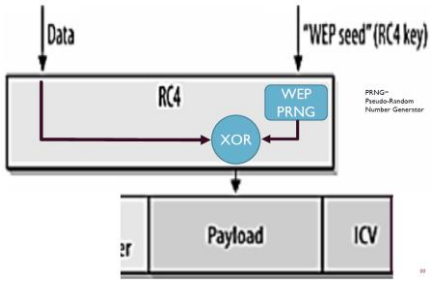




A partir del *payload* (campo de la trama) hay que calcular un CRC que se utilizará como ICV (Integrity Check Value) para detectar posibles modificaciones. El *payload* junto con el ICV forman el campo *data* que irá dentro del RC4.

Por parte del usuario tenemos definidas hasta cuatro claves para todos los usuarios (longitud 40, 104 o 232 bits) que se complementan con un IV (Initialization Vector) formando la *WEP seed*, también incluida en el RC4.

Este RC4 acaba conteniendo el payload y el ICV encriptados, siendo esto lo que se incluirá en la trama (primera imagen).



Viendo más a fondo el bloque RC4 vemos que a partir de la WEP seed se genera el keystream que hace el XOR con el campo *Data*, dando lugar al Payload encriptado.

¿En qué falló WEP?

Una única clave se utiliza para todo (cifrado, autenticación, confidencialidad) en todos los dispositivos y durante todo el tiempo. La gestión de estas claves es manual, el IV demasiado pequeño y la integridad CRC no es muy útil.

Para mejorar la seguridad con WEP podemos combinarlo con Open system, pero incluso así sigue siendo un mal sistema de seguridad, ya que es necesario conocer la clave para que el AP no descarte los paquetes que se le envíen.

La autenticación compartida tiene un fallo grave, ya que es un protocolo simple de desafío/respuesta. Es propenso a ataques de diccionario offline. Una clave WEP se expondría fácilmente. Además, incluso en la Autenticación abierta, un dispositivo que no

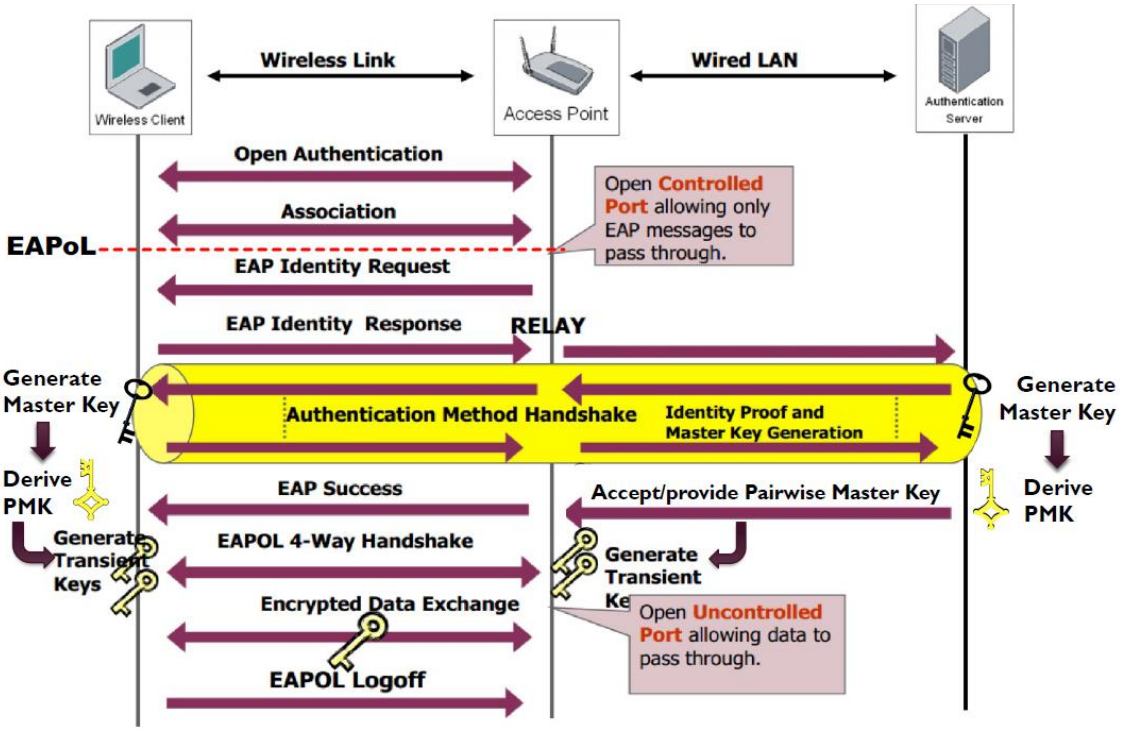
tenía la clave WEP no podría comunicarse a través del PA, ya que el AP descartaría todos los paquetes de datos del dispositivo. La compartida no añade seguridad y puede debilitarla. ¡WEP se conoció como **Worst Ever Privacy!**

¿Qué podemos hacer?

- Buscar los protocolos más adecuados para cada función, no intentar resolverlo todo a la vez.
- Cambiar las claves de forma automática y frecuente.
- Autenticar usuarios (no dispositivos) y redes, etc.
- Utilizar protocolos robustos para autenticación, integridad y confidencialidad:
    - **WPA** es un sustituto inmediato de WEP (mismo hardware que WEP) con cifrado TKIP, también basado en RC4. Autentificación 802.1X / PSK.
    - **WPA2** es más sofisticado. El hardware ya no es el mismo que WEP (más nuevo y potente) y el cifrado es CCMP (basado en AES). Autentificación 802.1X / PSK.

802.1X (EAP):

Cuando un cliente solicita ser autenticado el AP se conecta con un servidor de autenticación (RADIUS) que es el que valida la autenticación. Basado en el paradigma request/response. Es un método flexible a diferentes métodos de autenticación, especificables en el campo type de la trama.

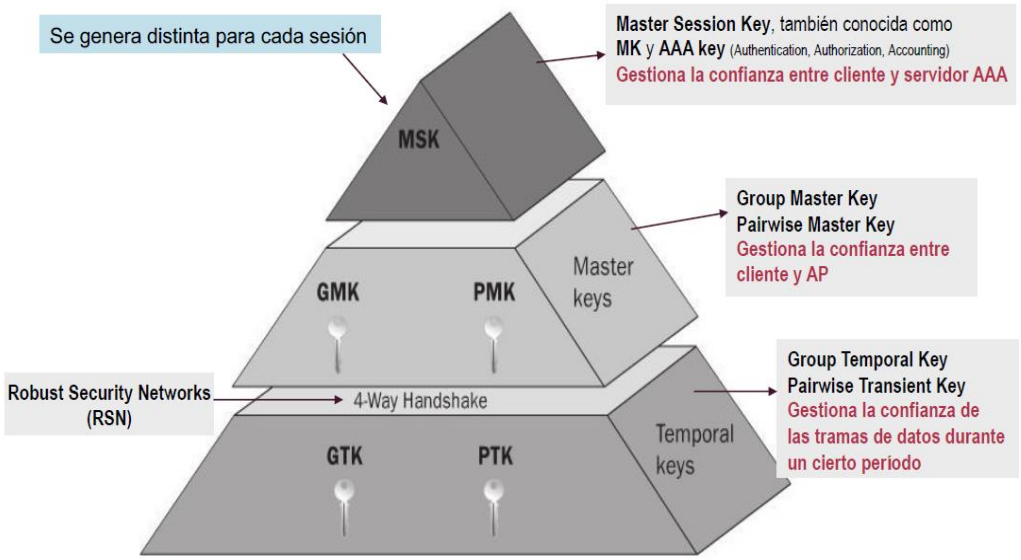


Inicialmente el cliente solo puede comunicarse con el Authentication server mediante mensajes. Una vez el protocolo EAP recibe el mensaje EAP del usuario, comienza el proceso de generación de claves.

A fin de establecer una conversación segura, tanto el cliente como el servidor RADIUS (authentication server) envían al otro una serie de valores *random* a partir de los cuales generan la misma **Master Key.**

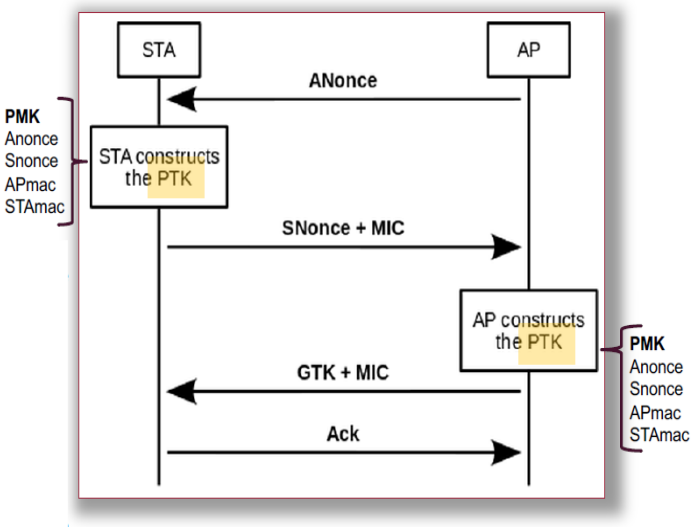
A partir de esta Máster Key consensuan una **Derive PMK**. El servidor RADIUS le enviará la suya al AP para que la utilice para cifrar sus comunicaciones con el cliente (única situación en la que se produce el envío de un clave).

A partir de la PMK se generarán las **Pairwise Transient Keys (PTK)**, que son las que se usarán para cifrar los datos enviados. Su tiempo de vida es muy limitado.



Las claves **GMK** y **GTK** están pensadas como claves grupales para cuando sea necesario hacer difusión por broadcast o multicast, para utilizar la misma *key* con un grupo de clientes.

Asociaciones Robust security networks (RSN): proceso para consensuar la PMK y a partir de ella generar la PTK. Se consigue mediante un intercambio de cuatro mensajes:



1. El AP genera y envía un ANonce, un numero aleatorio que se utilizará solo una vez.

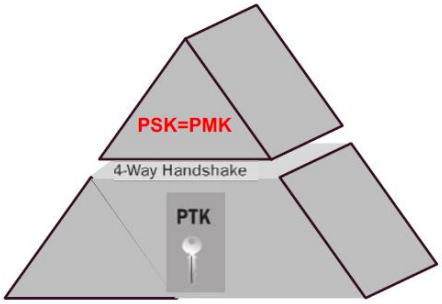
2. La estación construye la PTK a partir del Anonce y otros valores. Después envía al AP un SNonce junto con un código de integridad MIC para demostrarle al punto de acceso que conoce la PMK.

3. El AP recibe el mensaje y construye también la PTK. Después manda la GTK junto con otro MIC.

4. La estación responde con un ACK.

El servicio RADIUS. Es capaz de trabajar con distintos repositorios de cuentas de usuario (AD de Windows, LDAP…).

Puede existir una jerarquía de servidores RADIUS, *eduroam* es un ejemplo. Si nos vamos por ejemplo a Suiza y nos queremos conectar al servidor de la UPV (España), primero nos conectaremos al de Suiza (servidor RADIUS local) el cual subirá hasta el nivel más alto de la jerarquía y bajará buscando el servidor RADIUS de la UPV. Una vez encontrado establecerá un **canal cifrado (túnel TLS)** para establecer comunicación directa cliente – UPV.



Pre-shared Keys (PSK): Es el método paralelo a 802.1X (EAP), pensado para redes de uso personal. No existe servidor RADIUS (el autenticador es el AP) y la PMK es sustituida por una PSK que es igual para todos los usuarios. Se genera a partir de una **contraseña + SSID** a la que se le aplica el algoritmo Password Based Key Derivation Function (PBKDF2).

Un **ataque PSK** consistiría en:

1. A partir de un diccionario de contraseñas ir probándolas y combinándolas con el SSID (este es fácil de obtener) para generar PSKs.

2. Dado que toda la información de la asociación RSN es pública (salvo la PMK, que en este caso no hay), obtener el resto de los elementos utilizados para generar la PTK (ANonce, SNonce, AP MAC y Client MAC) y combinar con la PSK generada para generar posibles PTKs.

3. Generar PTKs hasta que se encuentre aquella que permite generar el mismo MIC que la estación está utilizando para comunicarse con el AP.

En el momento en el que se encuentre tendremos la contraseña, la PSK y la PTK que están siendo utilizadas. La defensa contra esto es utilizar contraseñas de gran longitud (>20 caracteres).

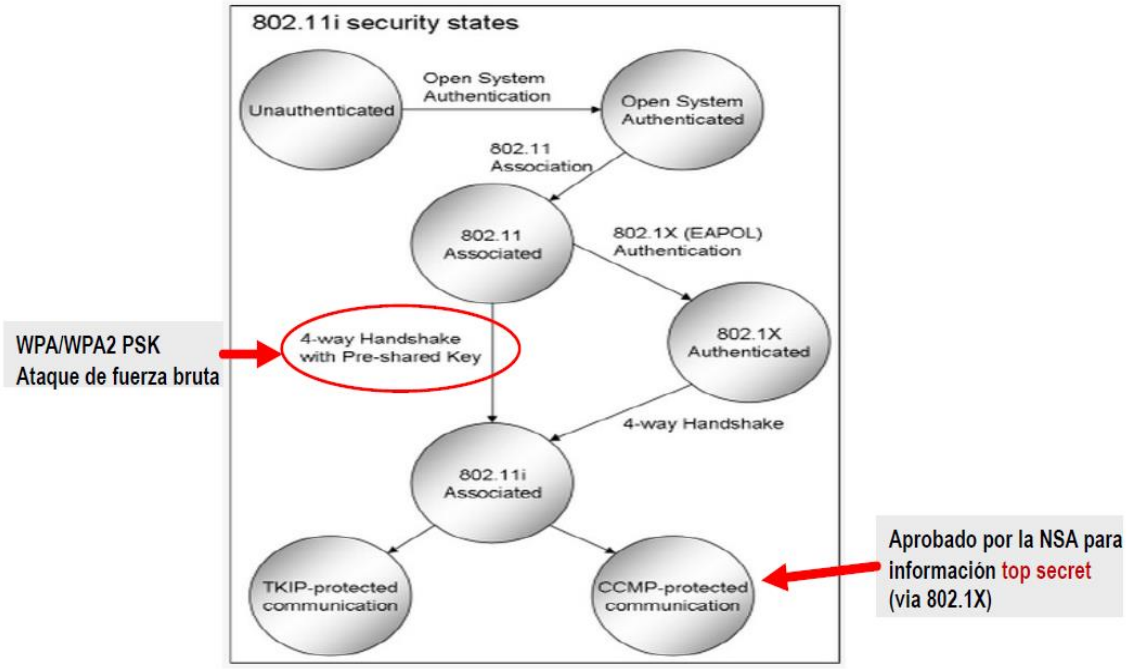
TKIP:

Introduce una serie de mejores respecto de WEP para WPA:

- El número de bits de los vectores de inicialización (IV) se duplica (de 24 bits **a 48 bits).**
- Cada conjunto de paquetes lleva asociada una clave distinta (en WEP se mantenía indefinidamente a menos que se cambiase de forma manual).
- Se utiliza un nuevo código de integridad MIC/Michael combinado con ICV que sustituye al CRC.

CCMP (COUNTER CIPHER MODE PROTOCOL)

Protocolo de cifrado estándar para WPA2. Se basa en el Counter Mode with CBC-MAC (CCM) del estándar **AES**, el cual es increíblemente seguro contra ataques de fuerza bruta, ya que las claves son de 128 bits como mínimo = 3.4 x 10^{38} combinaciones, lo que se traduce en 1 billón de billones de años necesarios para adivinar la correcta (aunque la computación cuántica reduce ese tiempo a horas o minutos).



Actualmente, WPA / WPA2 no se puede ROMPER criptográficamente. Sin embargo, en circunstancias especiales, como cuando se elige una **contraseña débil en WPA/WPA2- PSK,** es posible recuperar la contraseña mediante ataques de diccionario.

Comparativa entre tecnologías.

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-Bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-Based

WPA3

Fue anunciado en 2018. Simplifica la seguridad Wi-Fi y mejora la autenticación y la fuerza criptográfica. Uso de Protected Management Frames (PMFs).

- WPA3-Enterprise con claves de 128 bits (similar a WPA2).
- WP3-Enterpise de máxima seguridad (192 bits).
- WPA3-Personal (mejora WPA2 PSK utilzando el método SAE). Hay modo WPA3 Only si todos los dispositivos utilizan WP3 y Transition mode que también soporta WP2.
- WPA3-SAE: Introduce el importante cambio de que cada usuario tiene una PMK individual (ya no hay una para todos) que además es válida solo durante la sesión actual.

WIFI CERTIFICATION

Wi-Fi Alliance certifica el estándar Wi-Fi y los siguientes productos compatibles:

- IEEE 802.11 a/b/g/n/ac/ad-compatible.
- IEEE 802.11i usando WPA2 y EAP.
- Wi-Fi Protected Setup (WPS) simplifica la conexión de dispositivos.
- Wi-Fi Direct permite la compartición de medios.
- Wi-Fi Passpoint -> Conexión segura y sencilla a un hotspot.
- Wi-Fi Miracast permite la transmisión de vídeo.

Wi-Fi Protected Setup (WPS).

Facilita la conexión de clientes a APs, permite **REGISTRAR (PA)** que se encarga de generar y emitir las credenciales al **ENROLLE (CLIENTE)** que se vincule y se vuelve a conectar utilizando sus nuevas credenciales de autenticación.

Problemas de WPS:

- Creado por Wi-Fi Alliance, no por el IEEE.
- Fallo de diseño.
- Código de 8 dígitos se puede descifrar en 5.500 intentos (fácil de lograr con ataques automatizados).
- La única solución es apagar WPS en el router (muchos ni siquieran pueden apagarlo).
- Problema para PSK, pero no 802.1X.

Wi-Fi Direct.

Busca mejorar la conectividad de dispositivo a dispositivo (mejor que usar la operativa ad-hoc). Se basa en el modo IEEE 802.11, y permite a los dispositivos negociar quién se hará cargo de las funcionalidades tipo Soft-AP (software que convierte un Wi-Fi cliente en un punto de acceso). Los dispositivos Wi-Fi heredados pueden conectarse a Wi-Fi Direct y heredar todos los mecanismos mejorados de QoS, ahorro de energía y seguridad.

Grupos P2P. Los dispositivos Wi-Fi Direct, conocidos como P2P, se comunican mediante grupos P2P. Se dividen en:

Propietarios del grupo P2P: implementa la funcionalidad tipo AP en el grupo P2P.

Clientes P2P: actúan como clientes.

Cuando dos P2P se descubren, negocian sus roles para establecer un grupo P2P.

Creación de grupos.

1. Estándar: los P2P negocian el papel de P2P GO.
2. Persistente: hay información de seguridad precompartida disponible.
3. Autónomo: un P2P puede crear de forma autónoma un grupo P2P.

Wi-Fi Passpoint.

Conocido como Hotpost 2.0, adopta la 802.11u. Se elimina la necesidad de que los usuarios encuentren y autentiquen una red cada vez que se conectan. Es decir, automatiza todo el proceso tradicional, ofreciendo una conexión transparente entre Pas y dispositivos móviles y soporte para el nivel de seguridad más alto con WPA2.

Wi-Fi Miracast.

"Compartir una pantalla de ordenador portátil con el proyector de una sala de conferencias en tiempo real" por ejemplo. Solución para mostrar multimedia entre dispositivos sin problemas, sin cables, ni conexión de red. Permite enviar video HD de hasta 1080p y sonido envolvente 5.1.