

# Xarxes WIFI

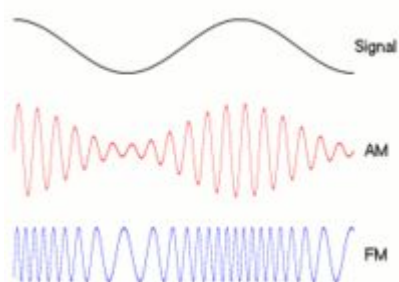
## Index

<a href="#"><u>Espectre radioelèctric</u></a>	<a href="#"><u>2</u></a>
<a href="#"><u>Regulació del espectre electromagnètic</u></a>	<a href="#"><u>2</u></a>
<a href="#"><u>Xarxes sense fils, conceptes bàsics</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>Configuracions per radiofreqüència</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>Bandes de freqüència</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>Banda d'ús comú i lliure</u></a>	<a href="#"><u>6</u></a>
<a href="#"><u>Assignació de canals</u></a>	<a href="#"><u>7</u></a>
<a href="#"><u>Modalitats</u></a>	<a href="#"><u>8</u></a>
<a href="#"><u>Protocols xarxa sense fils</u></a>	<a href="#"><u>9</u></a>
<a href="#"><u>Seguretat</u></a>	<a href="#"><u>10</u></a>
<a href="#"><u>Paràmetres bàsiques dels APs</u></a>	<a href="#"><u>14</u></a>
<a href="#"><u>Paràmetres bàsiques dels clients</u></a>	<a href="#"><u>14</u></a>

## Espectre radioelèctric

L'espectre radioelèctric (radiofreqüència, ones de ràdio o RF) és el conjunt d'ones electromagnètiques amb freqüències compreses entre 3 Hz i 3.000 GHz. Tots els sistemes de telecomunicació utilitzen senyals elèctrics per al transport de la informació.

Aquests es descriuen per la variació en el temps de les seves magnituds de tensió i corrent. A més d'aquesta descripció en el domini del temps, és possible establir-ne una altra en el domini de la freqüència, que és l'espectre del senyal. Cada mitjà de transmissió té el seu propi espectre radioelèctric o amplada de banda de transmissió en la qual s'ubiquen els senyals que s'hi propaguen.



## Regulació del espectre electromagnètic

Com que l'espectre radioelèctric és un bé limitat i sense possibilitat de créixer, es poden superposar un o diversos senyals diferents, però de la mateixa freqüència o molt propers, amb el risc de produir interferències i impedir l'establiment de cap comunicació.

És per aquesta raó que l'espectre radioelèctric adopta el caràcter de bé de domini públic i el seu control i custòdia passen a ser responsabilitat de les administracions públiques, les quals estableixen el reglament d'ús i l'assignació de freqüències i potències d'emissió per a les estacions i els serveis de comunicació que ho sol·licitin.

- **A nivell internacional**, l'organisme que s'encarrega de regular les telecomunicacions és la Unió Internacional de Telecomunicacions, una agència dependent de l'ONU integrada per 168 estats membres, en la qual els governs i el sector privat coordinen l'establiment i l'operació de xarxes de telecomunicacions i serveis, i es responsabilitzen de la reglamentació, l'estandardització, la coordinació i el desenvolupament de les telecomunicacions internacionals, com també de l'harmonització dels reglaments nacionals. El seu objectiu és fomentar i facilitar el desenvolupament global de les telecomunicacions per al benefici universal de la humanitat, mitjançant les regles de les lleis, el consens mutu i les accions cooperatives. La seva missió és proveir els productes i serveis necessaris per a tota la comunitat vinculada a les telecomunicacions, que una organització internacional sempre pot oferir de millor manera.

- **A nivell europeu**, hi ha l'European Telecommunications Standards Institute (**ETSI**), organisme que s'encarrega de generar les normes tècniques necessàries per aconseguir un mercat europeu de telecomunicacions ampli i unificat.
- **Dins l'estat espanyol**, els organismes reguladors de les telecomunicacions són el Ministeri d'Indústria, Turisme i Comerç (Direcció General de Telecomunicacions i Tecnologies de la Informació) i el Ministeri d'Educació i Ciència (Comissió del Mercat de les Telecomunicacions). Aquests ministeris gestionen la Llei General de Telecomunicacions, que és el marc legal de referència a la qual es refereixen els decrets llei i reglaments tècnics i que es va elaborar seguint les directives europees.

## Xarxes sense fils, conceptes bàsics.

Una xarxa d'àrea local sense fils, també coneguda com WLAN (de l'anglès wireless local area network), és un sistema de comunicació sense fils per minimitzar les connexions cablejades.

Utilitzant les ones de ràdio per portar la informació d'un punt a un altre sense necessitat d'un medi físic guiat. En parlar d'ones de ràdio ens referim normalment a portadores de ràdio, sobre les quals va la informació, ja que realitzen la funció de portar l'energia a un receptor remot. Les dades a transmetre es superposen a la portadora de ràdio i d'aquesta manera poden ser extrets exactament en el receptor final.

A aquest procés se l'anomena modulació de la portadora per la informació que està sent transmesa. Si les ones són transmeses a diferents freqüències de ràdio, diverses portadores poden existir en igual temps i espai sense interferir entre elles. Per extreure les dades el receptor se situa en una determinada freqüència, freqüència portadora, ignorant la resta.

En una configuració típica de LAN (amb cable) els punts d'accés connecten la xarxa cablejada d'un lloc fix mitjançant cablejat normalitzat. El punt d'accés rep la informació, l'emmagatzema i la transmet entre la WLAN i la LAN cablejada. Un únic punt d'accés pot suportar un petit grup d'usuaris i pot funcionar en un rang d'almenys trenta metres i fins a diversos centenars. El punt d'accés (o l'antena connectada al punt d'accés) és normalment col·locat en alt però podria col·locar-se en qualsevol lloc en què s'obtingui la cobertura de ràdio desitjada. L'usuari final accedeix a la xarxa WLAN a través d'adaptadors. Aquests proporcionen una interfície entre el sistema d'operació de xarxa del client (ENS: Network Operating System) i les ones, mitjançant una antena.

La naturalesa de la connexió sense cable és transparent a la capa del client.

## Configuracions per radiofreqüència

Poden ser de molt diversos tipus i tan simples o complexes com sigui necessari. La més bàsica es dona entre dos ordinadors equipats amb targetes adaptadores per WLAN,

## UF01

de manera que poden posar en funcionament una xarxa independent sempre que estiguin dins de l'àrea que cobreix cada un. Això és cridat xarxa d'igual a igual (peer to peer). Cada client tindria únicament accés als recursos de l'altre client però no a un servidor central. Aquest tipus de xarxes no requereix administració o configuració prèvia. [Veure exercici 1]

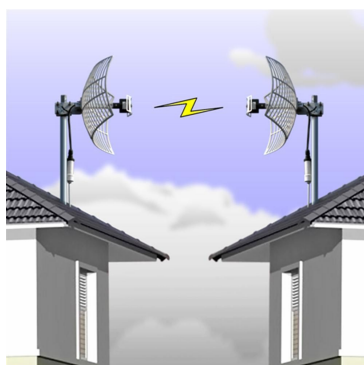
Instal·lant un Punt d'Accés es pot doblgar la distància a la qual els dispositius poden comunicar-se, ja que aquests actuen com a repetidors. Des que el punt d'accés es connecta a la xarxa cablejada qualsevol client té accés als recursos del servidor i a més gestionen el trànsit de la xarxa entre els terminals més pròxims. Cada punt d'accés pot servir a diverses màquines, segons el tipus i el nombre de transmissions que tenen lloc. Els punts d'accés tenen un abast finit, de l'ordre de 150 m en llocs o zones obertes. En zones grans com per exemple un campus universitari o un edifici és probablement necessari més d'un punt d'accés. La meta és cobrir l'àrea amb cèl·lules que solapen les seves àrees de manera que els clients puguin moure sense talls entre un grup de punts d'accés. Això és anomenat roaming.

Per resoldre problemes particulars de topologies, el dissenyador de la xarxa pot triar usar un Punt d'Extensió (EPs) per augmentar el nombre de punts d'accés a la xarxa, de manera que funcionen com a tals però no estan enganxats a la xarxa cablejada com els punts d'accés. Els punts d'extensió funcionen com el seu nom indica:

- Estenen l'abast de la xarxa retransmetent els senyals d'un client a un punt d'accés o a un altre punt d'extensió.
- Els punts d'extensió poden encadenar per passar missatges entre un punt d'accés i clients llunyans de manera que es construeix un pont entre tots dos.

Un dels últims components a considerar en l'equip d'una WLAN és l'antena direccional. Per exemple:

- Es vol una LAN sense cable a un altre edifici a 1 km de distància. Una solució pot ser instal·lar una antena en cada edifici amb línia de visió directa. L'antena del primer edifici està connectada a la xarxa cablejada mitjançant un punt d'accés. Igualment en el segon edifici es connecta un punt d'accés, la qual cosa permet una connexió sense cable en aquesta aplicació.



## Bandes de frecuencia

El Quadre Nacional d'Atribució de Freqüències (en endavant CNAF), peça bàsica de l'ordenament de l'espectre a Espanya, conté l'atribució o ús a què es reserva cadascuna de les bandes de freqüència en què es divideix l'espectre radioelèctric disponible per radiocomunicacions, entre 8,3 kHz i 3000 GHz.

El CNAF s'estructura en una primera columna amb una sèrie de taules que recullen l'atribució de bandes de freqüències segons l'article 5 del Reglament de Radiocomunicacions (RR) de la UIT, una segona columna amb les taules amb l'atribució nacional de cada banda de freqüències que excepte casos puntuals coincideix amb l'anterior. Una tercera columna es refereix al tipus d'ús de l'espectre que s'aplica a cada banda de freqüències, amb les següents modalitats:

- C: Ús comú
- E: Ús especial
- P: Ús privat
- R: Ús reservat a l'Estat
- M: Ús mixt que comprèn els usos P i R

[https://www.mincotur.gob.es/telecomunicaciones/espectro/CNAF/tablas\\_2017.pdf](https://www.mincotur.gob.es/telecomunicaciones/espectro/CNAF/tablas_2017.pdf)

<p>2300 - 2450 FJO MÓVIL Aficionados Radiolocalización</p>	<p>M M E R</p>	<p>5.150  UN-50, UN-51 Banda de aplicaciones ICM: 2400-2500 MHz UN-85, UN-86, UN-109, UN-115, UN-129, UN-154</p>	<p>pàg 68</p>
<p><b>4800 - 5570 MHz</b></p> <p>5460 - 5470 RADIONAVEGACIÓN EXPLORACIÓN DE LA TIERRA POR SATELITE (activo) INVESTIGACIÓN ESPACIAL (activo) RADIOLOCALIZACIÓN</p>	<p>R M M R</p>	<p>5.448B 5.448D 5.449  UN-145 TLPR UN-154</p>	<p>pàg 76-77</p>

## Banda d'ús comú i lliure

Com es pot veure en el quadre del CNAF un bon número de bandes estan regulades i/o assignades a empreses privades ( amb les seves limitacions d'ús com zona geogràfica, temps d'utilitat..).

Tal com s'estableix es disposa de les freqüència de baixa potència per trànsmissió d'aplicacions industrials, científics, mèdics, domèstics o similars, però no per la telecomunicació.

Per aquest motiu, es van establir les **freqüències de lliure utilització**. Aquestes freqüències les pot utilitzar qualsevol persona/entitat sense sol·licitar cap permís previ. Actualment, hi ha varies freqüències destinades a aquesta finalitat, però en concret parlarem de dues freqüències (pràcticament utilitzades a tot el món):

- 2,4 Ghz
- 5 Ghz

Per descomptat perquè això sigui possible és necessari complir amb certes regles que estan previstes en la regulació d'aquestes bandes. Les més importants tenen a veure amb la **potència màxima** i mecanismes per **evitar interferències**. A Europa, per a aplicacions d'interior aquestes bandes tenen una limitació de potència de 200 MW i per a exteriors de 1 W o 4 W depenent de la freqüència exacta. Aquestes potències són força baixes si les comparem amb les que radien les antenes de mòbils que poden arribar a ser de 25 W o més i per això cal anar amb compte en posar antenes molt grans als equips de WiFi per enllaçar dos punts allunyats.

Pel que fa a les interferències, la limitació de potència ja és en si un mecanisme per evitar interferències, però hi ha altres mecanismes com salts automàtics de canal que han de complir els equips que treballen en aquestes freqüències per poder operar.

La quasi totalitat de projectes que ens podem trobar amb companyies petites, en ajuntaments, ports, hospitals, etc. es fan en aquestes bandes lliures, perquè tots aquests organismes no tenen els mitjans, ni l'estatus legal per comprar una freqüència on desplegar el seu projecte; el cost seria impagable.

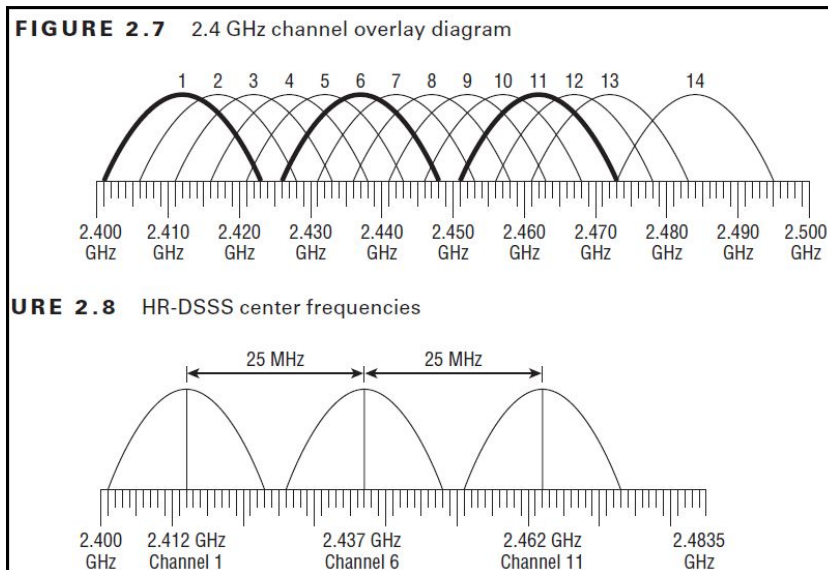
## Assignació de canals

Quan es va definir els dos rangs de freqüència lliure també es van definir les freqüències que es podrien utilitzar.

En el cas de 2,4 GHz es van establir 14 canals de 5MHz. Cada país té la possibilitat d'aplicar les seves pròpies restriccions sobre aquests 14 canals, per exemple USA només utilitza els 11 primers canals. El **problema** d'aquesta distribució és que cada canal necessita 22MHz per poder operar. Això el que provoca és que diversos canals quedin

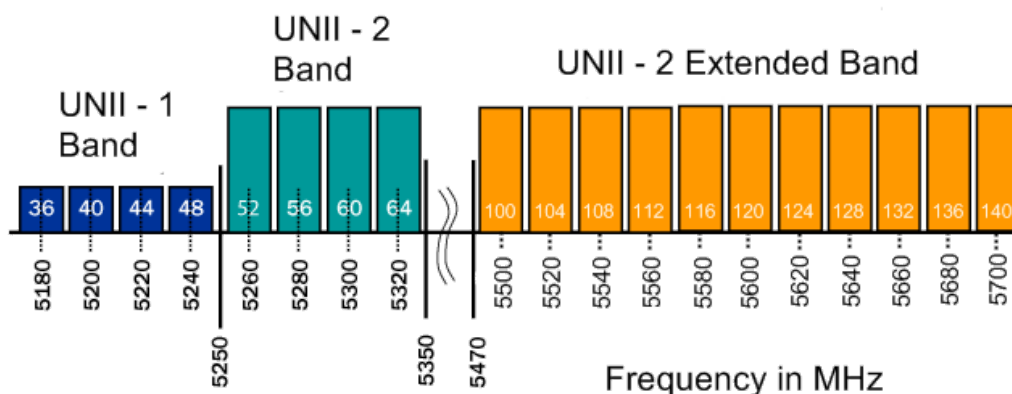
UF01

superposats. El concepte és important, perquè quan es produeix un superposició és possible que en la comunicació es produeixin problemes de comunicació.



En el cas de 5GHz es van establir varis canals dins de la freqüència delimitats per 20Mhz. Important comentar que des de la freqüència 5350 fins a 5470 no es possible utilitzar.

5.x GHz ISM Band: Channels [36,140] in North America & Europe



## Modalitats

### Wireless Access Point

En la creació de xarxes d'ordinadors, un punt d'accés sense fils (WAP), o, en general, només punt d'accés (AP), és un dispositiu de maquinari de xarxa que permet connectar un dispositiu Wi-Fi a una xarxa cablejada. L'AP sol connectar-se a un router (a través d'una

UF01

xarxa cablejada) com a dispositiu independent, però també pot ser un component integral del propi enrutador.



## Wireless Station Point

Un Wireless Station Point (estació/station) és una interfície sense fils que cercarà i posteriorment es connectarà a un AP (wireless access point). La connexió entre l'estació i el AP es comportarà de manera lleugerament diferent segons el mode d'estació que s'utilitzi.



## Protocols xarxa sense fils

L'estàndard IEEE 802.11 defineix l'ús dels dos nivells inferiors del model OSI (capa física i capa d'enllaç de dades), especificant les normes de funcionament d'una xarxa d'àrea local sense fil (WLAN). La primera versió de la norma es va publicar el 1997 per l'Institute of Electrical and Electronics Engineers o **IEEE**, el qual actualment s'encarrega del seu manteniment. Les especificacions d'aquest estàndard proporcionen la base per als productes amb xarxes sense fils que fan ús de la marca **Wi-Fi**.



Wi-Fi és una marca de l'Aliança Wi-Fi, l'organització comercial que adopta, prova i certifica que els equips compleixen amb els estàndards 802.11 relacionats amb xarxes sense fils d'àrea local. La seva primera denominació va ser "Wireless Ethernet Compatibility Alliance".



L'estàndard IEEE 802.11 es defineixen una sèrie de tècniques mitjançant l'aire que utilitzen 802.11. El primer estàndard, 802.11-1997 va ser canviat per 802.11-B, que va ser el primer àmpliament acceptat. Posteriorment, han sortit molts més estàndards acceptats per molts fabricants: 802.11a, 802.11g, 802.11n, 802.11ac.

	802.11a	802.11b	802.11g	802.11n	802.11ac
Any aprovació	1999	1999 (rectificació primer estandard)	2003	2004	2014
Freqüència d'ús	5Ghz	2,4Ghz	2,4Ghz	2,4Ghz i 5Ghz	5ghz
Velocitat teòrica de transmissió	54Mbit/s	11Mbit/s	54Mbit/s	600Mbit/s	1300Gbit/s
notes					Velocitat teòrica amb un ample de canal de 160Mhz (problemes de superposició)

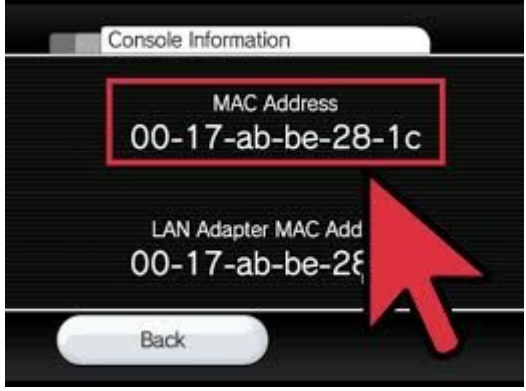

## Seguretat

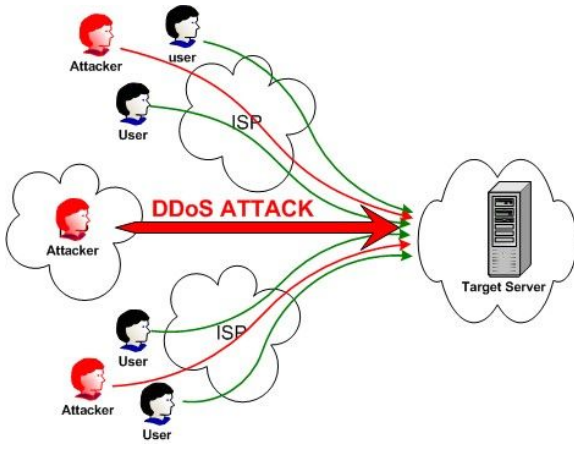
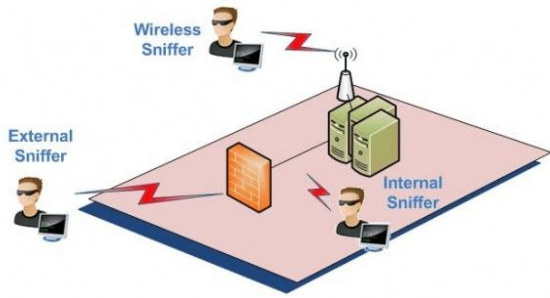
Els sistemes de transmissió de dades de forma inal·làmbrica són una gran eina, sobretot per la comoditat que generen en el moment de connectar-nos. Ens possibiliten poder tenir una connexió sense cables. Per tant, estalviant l'aprovisionament de cable. Ara bé, també són una font de problemes de seguretat. Recordem les seves característiques bàsiques que a la vegada formen part del seu portfolio de vulnerabilitats:

1. Operen a la Layer1 del model OSI, és a dir, entre station i acces point no hi ha un mitjà físic que ens garanteixi la correcta connexió i validació de receptor<->emissor.

- El estándar 802.11 no ha estat creat per ser segur, sino per transmetre amb bones velocitat. Això ha obligat a crear implementacions superior per evitar-ho.

## Llista de vulnerabilitats tíques dels accessos sense fils:

Identity theft (MAC spoofing)	<p>Un atacant, mitjançant eines especials, identifica una MAC d'un usuari amb privilegis per accedir a una xarxa inal·lambrica amb accés a la xarxa. Un cop ha aconseguit aquesta MAC pot suplementar l'identitat de l'altre equip i entrar en la xarxa especificada.</p> 
Man-in-the-middle	<p>Un atacant mitjançant un falç AP suplementa l'identitat d'un AP autentic. Un cop fet això, el atacant pot sniffar el tràfic de la xarxa obtenint tot el tràfic que no estigui degudament protegit.</p> 
Denial of service (DOS)	<p>Es produeix aquesta tipologia d'atac en el moment que un atacant envia molts paquets contra un AP. En aquest punt, es pot aconseguir saturar la connexió impedit que la resta d'usuaris puguin utilitzar la connexió.</p>

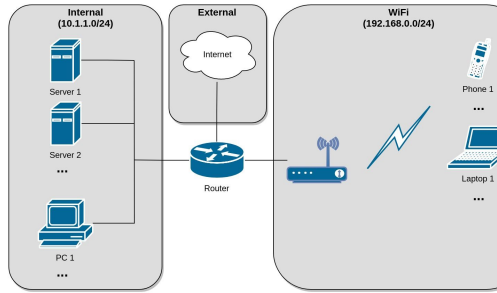
	
<p>Sniffer</p>	<p>Si la connexió no està degudament configurada, un atacant (un cop connectat al AP) pot realitzar un sniffer (captura de paquets).</p> 

## Mesures preventives de seguretat en xarxes sense fils

Per millorar la seguretat de les xarxes WIFI es poden implementar les següents mesures:

	Descripció	Inconvenients principals
SSID hiding	La majoria de fabricants permeten ocultar el SSID. Quan es realitza una ocultació del SSID les estacions no detecten la xarxa sense fils. Amb aquesta tècnica un atacant hi ha de conèixer el SSID del AP, no el pot obtenir de forma automàtica.	S'han de configurar totes les estacions de forma manual. Amb el cost de temps que suposa per part de l'administrador de sistemes.
Static IP	Es pot configurar la xarxa que utilitza el AP perquè no assigni IPs de forma dinàmica (DHCP).	S'han de configurar totes les estacions de forma manual. Amb el cost de temps que suposa per part

	D'aquesta forma un atacant ha de coneixer el rang i port d'enllaç de la xarxa.	de l'administrador de sistemes.
Access-List	El administrador de la xarxa limita mitjançant unes llistes d'accés quines MAC es poden connectar en els APs. D'aquesta forma només es connecten els equips que la seva MAC es coneguda	S'han de configurar totes les Access-List de forma manual. Amb el cost de temps que suposa per part de l'administrador de sistemes.
802.11 security	<p>És un estàndard de la IEEE per garantir el correcte registrament de nous equips a la xarxa sense fils mitjançant una <b>autenticació</b> (contrasenya). Els més típics són:</p> <ol style="list-style-type: none"> <li>1. <b>WEP.</b> En via d'extinció, ja que el 2007 es va demostrar que era complement insegur. Han sortit moltes eines que en pocs minuts es capaç de trencar la seva seguretat.</li> <li>2. <b>WP &amp; WPA2:</b> Actualment aquest metodes també estan compromesos. La forma més comuna d'atac és mitjançant <i>force brute</i>. El atacant va provant multiples conuinacions de contrasenyes fins trovar la correcta. Aquesta vulnerabilitat es fàcil de combatre amb contrasenyes robustes. També s'han descobert altres vulnerabilitats, tot i que s'han corregit llançant millores en el estàndard.</li> <li>3. <b>WPA3:</b> Millora l'implementació de seguretat, amb contrasenyes més robustes. Té l'inconvenient que station i AP han de implementar-la.</li> </ol>	Aquesta mesura de seguretat només té el inconevint de que les contrasenyes es poden traspasar sense el consentiment del administrador.
Client Forward	Activant aquesta mesura de seguretat es garanteix que una	El AP ha d'incloure aquesta funcionalitat.

	station connectada a la xarxa no podrà veure el tràfic de les altres stations	Activant aquesta funció les stations que necessitin rebre tràfic broadcast o multicast no funcionaran. Un exemple a nivell domèstic és l'ús d'aparells com el Chromecast.
Mínima exposició	En els muntatges empresarials és convenient exposar el mini'm possible de la xarxa interna mitjançant els accessos sense fils. Un bon exemple, seria la limitació de la xarxa "invitats". Una xarxa on es pot connectar qualsevol una bona mesura seria limitar l'exposició d'aquesta xarxa i només oferir accés a Internet, sense accés als actius interns.	<p>Bon coneixement de la xarxa interna. Potser possible que els clients usuaris d'aquesta xarxa limitada necessitin més accessos en tal cas s'hauria de muntar un segon AP o excloure aquest equip de les regles de firewall</p> 

## Paràmetres bàsiques dels APs

A continuació es llisten les principals característiques i paràmetres de configuració d'una xarxa WIFI. Pot ser que un fabricant concret ens faciliti menys paràmetres o bé paràmetres diferents, però aquests serien els bàsics que s'hi haurien de conèixer:

- **Modalitat [AP / station]:** Configuració del aparell per treballar amb mode AP o bé mode estació.
- **Virtual AP:** Mitjançant només una interface es pot crear multiples SSID. Amb aquesta modalitat pots reutilitzar canals i no és necessari adquirir nous equips.
- **Amplada del canal:** Normalment és treballa a 20MHz tal com s'ha explicat anteriorment, però alguns equips permeten ampliar l'amplada del canal. Alerta, ampliar l'amplada del canal pot favorir a tenir problemes d'interferències.
- **Freqüència/canal:** Selecció del canal on es vol treballar. Per exemple 5180 o 5700
- **SSID (Service Set Identifier):** és el nom que identifica una xarxa sense fil WIFI i el que viatja juntament amb cada paquet d'informació de la mateixa, de manera que es pugui identificar com a part d'ella.
- **Protocol:** selecció de tots els protocols 802.11
- **País:** Important determinar en quin país està actuant el AP. Segones el país alguns canals no estaran disponibles.

UF01

- **DFS activat:** Permet als dispositius de 5Ghz que treballen amb l'estàndard 802.11 compartir l'espectre amb radars. Aquests radars són utilitzats en aeroports, estacions meteorològiques i militarment.
- **Potència d'emissió:** Configuració de la potència en la que treballa el AP. Aprx. 200 MW i per a exteriors de 1 W o 4 W.
- **Protocol seguretat:** Configuració del estàndard 802.11-security.

## Paràmetres bàsiques de la connexió de les estacions

A continuació es llisten les principals característiques i paràmetres de connexió d'una xarxa WIFI en mode station. Pot ser que un fabricant concret ens faciliti menys paràmetres o bé paràmetres diferents, però aquests serien els bàsics que s'hi haurien de conèixer:

- **Uptime:** temps que porta l'estació connectada al AP.
- **TX/RX signal:** Tx és la potència en decibels (dBm) en què un AP transmet el seu senyal. El nivell Rx és la potència en dBm del senyal rebut. Es mesuren amb quantitats negatives, per tant, com més propers a 0 més intensitat de senyal és rebrà/transmetrà. Un excés d'intensitat pot portar interferències.
- **CCQ:** La qualitat de la connexió del client (CCQ) és un valor en percentatge que mostra l'efectivitat de l'ample de banda en relació amb l'amplada de banda disponible en el màxim teòric. CCQ és una mitjana ponderada de valors  $T_{min} / T_{real}$ , que es calcula per a cada fotograma transmès, on  $T_{min}$  és el temps que trigaria a transmetre el marc donat a la major velocitat sense reintents i  $T_{real}$  és el temps que va trigar a transmetre el marc a la vida real recomptes necessàries necessàries per transmetre velocitat de transmissió i transmissió).