



Escola Universitària
Politècnica de Mataró

Enginyeria Tècnica de Telecomunicació, especialitat Telemàtica

ENTORN PRÀCTIC DE WIFI

Frederic Monpeat i Santo

Primavera 2007



Escola Universit ria
Polit cnica de Matar 

Enginyeria T cnica de Telecomunicaci , especialitat Telem tica

ENTORN PR CTIC DE WIFI

Frederic Monpeat i Santo

Antoni Satu  Villar

Primavera 2007



Escola Universit ria
Polit cnica de Matar 

Enginyeria T cnica de Telecomunicaci , especialitat Telem tica

TREBALL FI DE CARRERA

T TOL:

AUTOR:

PROFESSOR PONENT:

QUALIFICACI 

Defensat el treball en la convocat ria del dia: ____ de _____ de ____.

Ha obtingut la qualificaci  de

Director
EUPMt

Professor
Delegat UPC

Professor
Ponent

.....

.....

.....

Secretari

.....



[Creative Commons](#)

Creative Commons License Deed

Reconeixement-NoComercial-CompartirIgual 3.0 No adaptada (CC BY-NC-SA 3.0)

Això és un resum fàcilment llegible del [text legal \(la llicència completa\)](#).
[Advertiment](#)

Sou lliure de:



copiar, distribuir i comunicar públicament l'obra



fer-ne obres derivades

Amb les condicions següents:



Reconeixement — Heu de reconèixer els crèdits de l'obra de la manera especificada per l'autor o el llicenciador (però no d'una manera que suggereixi que us donen suport o rebeu suport per l'ús que feu l'obra).



No comercial — No podeu utilitzar aquesta obra per a finalitats comercials.



Compartir Igual — Si altereu o transformeu aquesta obra, o en genereu obres derivades, només podeu distribuir l'obra generada amb una llicència idèntica a aquesta.

Entenent que:

Renuncia — Es pot [renunciar](#) a alguna d'aquestes condicions si obteniu el permís del titular dels drets d'autor.

Domini Públic — Aquesta llicència no afecta a la situació de l'obra o algun dels seus elements quan es trobi en el [domini públic](#), segons la llei vigent aplicable.

Altres drets — Els drets següents no queden afectats de cap manera per la llicència:

- Els vostres drets de repartiment just o [ús just](#);
- Els drets [morals](#) de l'autor;
- Drets que altres persones poden ostentar sobre l'obra o sobre l'ús que se'n fa, com per exemple drets [de publicitat](#) o privacitat.

- **Avís** — Quan reutilitzeu o distribuïu l'obra, heu de deixar ben clar els termes de la llicència de l'obra.

Dedicatòria

A la meva mare i al meu pare, allà on sigui, sempre amb mi.

Agraïments

La realització d'aquest projecte no hauria estat possible sense la dedicació de tots aquells que d'una manera o altre aporten en el seu temps i el seu coneixement a les xarxes sense fils, a tots els que comparteixen el seu saber amb els altres amb l'objectiu de no estar inventant la roda que diria aquell.

A les Comunitats sense fils i als que treballen dia a dia amb projectes com Mataró SenseFils on més enllà dels aspectes tècnics, s'utilitza el *WiFi* per unir a persones. A la EUPMt i la Associació d' Alumnes pel suport alhora de posar en marxa un projecte com Mataró Wireless. Però sobretot als companys de Mataró Wireless els quals dia a dia t'inspiren amb les seves idees, coneixements i sobretot passió per la tecnologia.

Als companys projectistes per aquest “estrés compartit” que tant ens uneix en un treball com aquest, a la meva família i amics per la comprensió tinguda, a la ciutat de Dublín per acollir-me en la major part de la realització d'aquest projecte i a la Duna per ajudar-me a “desestressar-me”.

A en Lèonard Janer pel suport i guionatge mostrat durant tots aquests anys en les diferents iniciatives de *WiFi* que s'han dut a terme i que en part han desembocat en aquest treball. També perquè junt amb en Pere Barberán m'han donat totes les facilitats possibles per la realització d'aquest projecte. I en el meu ponent, en Antoni Satué, per la confiança mostrada durant el tutelatge d'aquest projecte dut a terme en unes condicions tant poc habituals.

Finalment a la Justys pel seu suport i ànims constants en els moments més desesperants, fent-me sempre costat amb un somriure.

A tots, moltes gràcies, de veritat.

Resum

“Entorn pràctic de WiFi” és una visió de la tecnologia 802.11 des del punt de vista pràctic. El principal objectiu és oferir un document d'on en puguin sorgir unes pràctiques docents que permetin aprofundir en els aspectes teòrics, sempre des d'un punt de vista pràctic posant èmfasi en el funcionament de la tecnologia.

El treball està organitzat en un conjunt d'exercicis pràctics que, partint d'un coneixement mínim de la tecnologia WiFi, ens hi introdueix fins a un nivell avançat. Tot amb el mínim de material possible i amb eines de programari lliure les quals ens deslliguen d'uns equips concrets.

Resumen

“Entorno práctico de WiFi” es una visión de la tecnología 802.11 desde el punto de vista práctico. El principal objetivo es ofrecer un documento que pueda derivar en unas prácticas docentes que permitan profundizar en los aspectos teóricos, siempre desde un punto de vista práctico enfatizando en el funcionamiento de la tecnología.

El trabajo está organizado en un conjunto de ejercicios prácticos que, partiendo de un conocimiento mínimo de la tecnología WiFi, nos introduce hasta un nivel avanzado. Todo con el mínimo de material posible y con herramientas de programario libre las cuales nos desvinculan de equipos concretos.

Abstract

“Practical WiFi Environment” is a vision of 802.11 technology from a practical point of view. The main target is to introduce a document which can become in academic exercises. The idea is to study the theoretical concepts from the practical point of view, emphasizing how it works the technology.

The project has a group of practical exercises which goes from basic knowledges to advanced, only with minimum devices and with Free Software which is possible to work with a lot of hardware.

Índex

Capítol I: Introducció.....	1
Capítol II: Objectius.....	3
Capítol III: Configuració bàsica d'una xarxa <i>WiFi</i>.....	5
Introducció al WiFi.....	5
Configuració d'un Punt d' Accés.....	7
Conceptes teòrics.....	7
Objectiu.....	8
Realització.....	9
Configuració del Client: <i>Wireless Extensions – Wireless Tools</i>	11
Conceptes teòrics.....	11
Objectiu.....	12
Realització.....	13
Paràmetres d'enllaç: <i>Link Quality Anàlisi (LQA)</i>	15
Conceptes teòrics.....	15
Objectiu.....	20
Realització.....	20
Modes de connexió: <i>Ad-Hoc</i> i <i>Infraestructura</i>	26
Conceptes teòrics.....	26
Objectiu.....	28
Realització.....	28
Capítol IV: Paràmetres de Seguretat.....	29
Seguretat elemental: CNAC i ACL.....	29
Conceptes teòrics.....	29
Objectiu.....	30
Realització.....	30
Encriptació de Dades: WEP.....	37
Conceptes teòrics.....	37
Objectiu.....	39
Realització.....	39
Autenticació. <i>Open System</i> i <i>Shared Key</i>	42
Conceptes teòrics.....	42
Objectiu.....	44
Realització.....	44

Encriptació Avançada: WPA/WPA2.....	50
Conceptes teòrics.....	50
Objectiu.....	54
Realització.....	55
Capítol V: Anàlisi dels paquets.....	61
Descripció dels paquets.....	61
Tipus de paquets.....	61
Anàlisi d'un <i>Beacon Frame</i>	68
Vulnerabilitats.....	77
Esbrinar SSID Ocults (CNCP).....	77
Esbrinar MAC permeses (ACL).....	78
Esbrinar la clau de cifratge (WEP).....	79
Capítol VI: Conclusions.....	83
Bibliografia.....	85
Apèndix A: Manuals.....	87
Apèndix B: Article “Insurrección Wireless”.....	101

Índex de imatges

Imatge 1. Opcions bàsiques d'un Punt d' Accés

Imatge 2. Xarxa Ad-Hoc

Imatge 3. Xarxa en mode Infraestructura

Imatge 4. Configuració del SSID Broadcast (Beacon Frames) en el Punt d'Accés

Imatge 5. Deshabilitem els Beacon Frames

Imatge 6. Opcions de restriccions ACL en el Punt d'Accés

Imatge 7. Llistat d'adreces MAC a filtrar

Imatge 8. Opcions de restriccions ACL en el Punt d'Accés Permit-Only

Imatge 9. Llistat d'adreces MAC a filtrar

Imatge 10. Encriptació WEP

Imatge 11. Desencriptació WEP

Imatge 12. Configuració WEP-64 del Punt d' Accés

Imatge 13. Configuració WEP-128 en el Punt d' Accés

Imatge 14. Opcions avançades del Punt d'Accés

Imatge 15. Opcions de seguretat del Punt d'Accés (WPA)

Imatge 16. Opcions de seguretat del Punt d'Accés (WPA2)

Imatge 17. Opcions de seguretat del Punt d'Accés (Mode Mixt)

Imatge 18. Analitzador WireShark

Imatge 19. Analitzador WireShark (Interfícies)

Imatge 20. Analitzador WireShark (Filtres)

Imatge 21. Analitzador WireShark (Paquets)

Índex de taules

Taula 1. Característiques generals dels protocols 802.11

Taula 2. Taula de Modulació en funció del bitrate i el protocol

Capítol I: Introducció

En els darrers anys hem pogut veure l'evolució que han sorgit les xarxes sense fils, sobretot al que coneixem sota la marca *WiFi*. A poc a poc s'han anat veient les avantatges a nivell de comoditat i facilitat que presenten aquest tipus de connexions. La ràpida evolució de l'estàndard oferint prestacions similars a les xarxes cablejades, el descens considerable en els preus dels equips i sobretot la flexibilitat que presenten aquest tipus de xarxes, han convertit a les xarxes *WiFi* en un concepte obligat per a qualsevol enginyer de xarxes.

Al llarg de la carrera d'enginyeria telemàtica podem trobar referències teòriques a aquests tipus de xarxes, a nivell de transmissió de dades, de coneixement general de xarxes o més específic en l'assignatura de “Comunicacions sense fils”. Malgrat tot el punt de vista és exclusivament teòric, fet que pot fer perdre interès a aquest tema tant apassionant.

Per altre banda existeixen cursos específics de *WiFi* però acostumen a ser de fabricants, entrant en més detall en les funcionalitats dels seus equips que no pas en el funcionament de la tecnologia. Acostumen a parlar de configuracions de xarxes *WiFi* amb determinats equips orientats de manera que aprengui el funcionament dels equips més que la lògica de la tecnologia. De manera que per la gent autodidacta és difícil trobar un curs de *WiFi* eminentment pràctic que t'introdueixi dins de la tecnologia.

Durant els darrers 5 anys he participat en el desenvolupament i promoció de xarxes i comunitats *WiFi*. En els primers anys la principal tasca va ser donar a conèixer la tecnologia. Havíem de convèncer a la gent que comencés a fer ús de la tecnologia i que a més participés en els projectes de construir una xarxa ciutadana. Ho vàrem fer mitjançant xerrades i tallers, on les presentacions donant a conèixer la tecnologia feia que els més inquiets s'interessessin per la tecnologia. Malgrat tot, els interessats sempre acabaven sent el mateix perfil de persona de manera que al final arribàvem només a un grup molt reduït de gent.

També resultava que les característiques més interessants de les xarxes *WiFi* es podien treballar perfectament en entorns GNU/Linux. Les presentacions es feien sobre

aquest entorn, les demostracions, els exemples i les proves. La gent sortia engrescada però al arribar a casa i provar-ho la majoria no se n'ensortia. Potser a la presentació es definien conceptes i es podien entendre, però després altres aspectes més bàsics com fer un scan del medi o simplement canviar el mode d'una targeta impediend que la persona pogués implementar aquells coneixements. Per tant tenim 3 factors importants:

- Visió exclusivament teòrica de la tecnologia.
- Impossibilitat de plantejar unes pràctiques vàlides per a qualsevol equip.
- Necessitat d'aprofundir més en les eines *WiFi*.

De tot plegat i després de consultar amb el ponent, sorgeix la idea de dissenyar un projecte que pugui esdevenir en unes pràctiques per aplicar en un entorn real: l'assignatura de “Comunicacions sense fils”. I no només amb aquesta finalitat sinó que a més puguin donar cabuda a les formacions de *WiFi* de Mataró Wireless.

La idea és doncs plantejar una formació en la tecnologia *WiFi* fonamentada amb el que es pot fer amb un Punt d'Accés domèstic i dues targetes. Expliquem l'estàndard i el seu desenvolupament sota la perspectiva del que més tard podem implementar en forma d'exercicis. A més defugim d'aplicacions propietàries i de sistemes de pagament: tot es realitza en entorn *GNU/Linux*. L'objectiu és doncs treure el màxim rendiment i aprofundiment dels conceptes en una comunicació *WiFi*, basat en el que especifica l'estàndard i sobretot en el que es pot fer amb les eines que disposem. Tot partint de la base que l'usuari no disposa de coneixements de la tecnologia i un nivell bàsic de *GNU/Linux* i de xarxes. Els diferents temes estan enfocats partint de 0, és a dir, definint els paràmetres bàsics per establir un xarxa, per més tard anar provant les diferents opcions de la tecnologia i veure que passa. Les opcions es tracten a nivell de configuració, interpretació de la informació que rebem, consells i detalls a tenir en compte alhora del disseny i muntatge i finalment com es realitza la comunicació per paquets. Bàsicament es tracten els paràmetres bàsics de configuració i la seguretat. En el treball no s'hi trobem configuracions avançades ni implementacions que no siguin estrictament de *WiFi*. Només s'hi tracten estàndards aprovats: 802.11a, 802.11b i 802.11g (no s'hi troben *drafts* de 802.11n o *MiMo*). Tampoc és un recull de vulnerabilitats i atacs a xarxes sense fils, tot i que també s'hi tracten, però en menor mesura.

En definitiva el que hi trobem és una visió àmplia i detallada de les possibilitats de la tecnologia tenint en compte que tot es pot fer amb un Punt d' Accés i dues targetes.

Capítol II: Objectius

L'objectiu principal és proporcionar el material necessari perquè en puguin sorgir unes pràctiques de *WiFi*, tenint en compte les següents premises:

- No ha de ser teòric: si ve és cert que hi han d'haver-hi conceptes teòrics, s'ha de poder assimilar mitjançant implementacions pràctiques tot el que s'explica.
- Ha d'anar orientat a un perfil d'estudiant que no disposa de coneixements de *WiFi*.
- Ha de poder-se realitzar amb el mínim de material.
- Ha de poder realitzar-se amb independència dels equips.
- Ha de donar una visió àmplia de les possibilitats de la tecnologia.

A nivell personal, els objectius són:

- Que es pugui realitzar amb programari lliure.
- Dificultat mínima en les configuracions.
- Donar una visió diferent del que es pot trobar respecte a formacions *WiFi*.

Capítol III: Configuració bàsica d'una xarxa WiFi

3.1. Introducció al WiFi

WiFi (acrònim de *Wireless Fidelity*) és una marca que defineix un conjunt d'estàndards de comunicacions per a xarxes locals sense fils (WLAN). Es basa en el conjunt de protocols oberts nomenats 802.11 i establerts per el IEEE.

A l'any 1997 va sorgir el primer text que definia el 802.11, una forma de comunicació mitjançant radiofreqüència que donava velocitats entre 1-2 Mbps i que permetia mobilitat. Però potser el factor més destacat era el fet que no es necessitava llicència per realitzar comunicacions ja que treballava en bandes de freqüència lliures. A l'any 1999 va aparèixer 802.11a el qual opera en la banda dels 5 Ghz i pot transmetre a un velocitat màxima de 54Mbps. Al mateix temps va aparèixer el 802.11b, el qual opera en els 2,4GHz (una banda menys sensible a les interferències i en la que es necessita menys potència de transmissió). Tot i disposar d'una velocitat menor 11Mbps, el seu èxit va ser determinant per l'avenç de les comunicacions sense fils. Això va ser degut a que 802.11a treballa en una banda de freqüència alta modulant amb OFDM el qual permet majors velocitats, però la seva capacitat de penetració resta molt reduïda a la mínima obstrucció. 802.11b utilitza una extensió de DSSS (*Direct Sequence – Spread Spectrum*) CCK (*Complementary Code Keying*) per a la modulació i treballa en una banda intermitja. No només es desenvolupa millor ens espais reduïts amb obstacles que els seu homònim 802.11a, si no que a més es van abaratir els costos dels dispositius. En canvi la velocitat és quasi un cinquena part de la aconseguida en 5 Ghz.

Malgrat tot amb el temps es van anar veient carències en la potència radiada efectiva del 802.11b, fet que el feien descendir la velocitat en entorns amb interferències o subjectes atenuacions. Estem parlant d'una banda lliure on dispositius com microones, comandaments a distància i d'altres aparells domèstics emeten. Tot plegat converteix la banda dels 2.4 Ghz en la més explotada. Degut a aquest fet, els mateixos fabricants van anar creant les seves pròpies extensions per intentar solucionar aquests problemes fins que al 2003, degut en part a aquestes millores aportades, apareix el 802.11g.

Permet arribar fins als 54 Mbs, connectar major nombre d'usuaris, és també robust davant les obstruccions i treballa a la mateixa banda que el 802.11b. Això li permet obtenir compatibilitat, aprofitar les seves avantatges i heretar del 802.11a OFDM per modular en els 6-9-12-18-24-36-54 Mbps. Ens els 5,5 i 11 Mbps treballa amb DDDS (CCK) com 802.11b i per sota amb DBPSK/DQPSK+DSSS.

Tot plegat el converteixen amb un protocol força robust però continua tenint els mateixos problemes que 802.11b: l'ocupació massiva de dispositius en els 2,4 Ghz eleva les possibilitats d'interferència.

Des del 2004 s'està treballant amb 802.11n el qual sembla que aportarà millores substancials als problemes de 802.11g. Per una banda es preveu que treballarà tant a la banda dels 2,4 Ghz com els 5 Ghz (multibanda). Utilitzarà la tecnologia MIMO (*Multiple Input – Multiple Output*) la qual utilitza un conjunt de micro-antenes amb la capacitat d'oferir múltiples connexions en canals diferents simultàniament, el que es tradueix en major velocitat (fins a 248 Mbps) i menor risc d'interferència. Malgrat aquestes expectatives tant esperançadores, la realitat és un altre. L'aparició de l'estàndard definitiu s'ha ajornat dues vegades i els fabricants semblen no posar-se d'acord en les especificacions. Això ha fet aparèixer al mercat models amb diferents denominacions (Pre-N, MiMo...) els quals es refereixen al *draft* del futur estàndard encara no finalitzat.

Dins del 802.11 trobem fins a 22 variants en les quals estan finalitzades o bé s'hi està treballant, a part de 2 reservades per possibles ús. D'aquestes variants a part de les ja esmentades, caldria mencionar al 802.11i el qual intenta donar solució a les deficiències de seguretat trobades amb les definides als estàndards previs. 802.11i apareix al 2004 junt amb 802.11g i es presenta com un conjunt de mesures adoptades per donar solució a les diferents vulnerabilitats trobades en la encriptació mitjançant WEP i als processos d'autenticació. En aquest nou recull trobem un conjunt de mesures com són 802.1x per l'autenticació, *Robust Security Network* (RSN) per les associacions i *Advanced Encryption System* (AES) per l'encriptació.

3.2. Configuració d'un Punt d' Accés

3.2.1. Conceptes teòrics

Els paràmetres bàsics que s'han d'especificar per dissenyar una xarxa *WiFi* són:

- **SSID (*Service Set Identifier*):** Identificador del conjunt de serveis o, dit altrament, nom de la xarxa . S'utilitza per diferenciar la nostra xarxa de les altres. Es compon de caràcters alfanumèrics i la seva extensió no pot excedir els 32 caràcters. El nom de la xarxa és a més *case Sensitive* pel que diferencia entre majúscules i minúscules. Podem trobar diferents denominacions més específiques per a referir-se al SSID, en funció del tipus de xarxa que volem desenvolupar.
- **BSSID (*Basic Service Set Identifier*):** és el SSID que denomina tota l'àrea de cobertura d'un Punt d' Accés.
- **ESSID (*Extended Service Set Identifier*):** en una xarxa estesa, és l'àrea de cobertura formada pel conjunt de BSSID.
- **IBSSID (*Independent Basic Service Set Identifier*):** en les connexions *Ad-Hoc*, cada node és una sola àrea de cobertura.

El SSID normalment s'emet constantment dins d'uns paquets anomenats *Beacon Frames* i que serveixen per facilitar la connexió a la xarxa. Habitualment en el Punt d' Accés trobem la opció d'emetre'ls o no. El fet de no emetre'ls fa que un usuari per connectar a la xarxa hagi de conèixer prèviament el nom d'aquesta per accedir-hi. Però cal remarcar que el SSID no és un *password*, és només l'identificador.

- **Protocol:** habitualment els Punts d' Accés ens permeten implementar xarxes on es pugui treballar amb més d'un protocol a la vegada. Depenent del nivell de sofisticació del nostre aparell, podrem escollir entre 1 o més protocols, amb l'opció de treballar amb més d'un simultàniament.

Protocol	Any d'aparició	Freqüència	Velocitat Real	Velocitat Teòrica	Cobertura Interior	Cobertura Exterior
Legacy	1997	2.4-2.5 GHz	0.7 Mbit/s	2 Mbit/s	~25 metres	~75 metres
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	23 Mbit/s	54 Mbit/s	~30	~100
802.11b	1999	2.4-2.5 GHz	4 Mbit/s	11 Mbit/s	~35	~110
802.11g	2003	2.4-2.5 GHz	19 Mbit/s	54 Mbit/s	~35	~110
802.11n	2007 (TGn draft 2.0) Previst 2008	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s	~70	~160

Taula 1. Característiques generals dels protocols 802.11

Les opcions actualment poden ser: 802.11a, 802.11b, 802.11g, 802.11pre-n o un mode mixt. Normalment es combinen les opcions en funció de les ràdios de l'aparell:

- **Ràdio de 2,4 Ghz:** és probable que pugui treballar amb B, G i pre-N.
- **Ràdio de 5 Ghz:** l'equip treballarà amb A.

Hi han equips que treballen amb dues ràdios pel que suporten les dues bandes de freqüència. També hi ha equips que suporten més d'un estàndard però d'una sola freqüència i hi ha equips que només poden treballar amb un estàndard (els més antics).

- **Canal o Freqüència:** en funció del protocol triat podrem seleccionar un dels canals pels quals estigui permès emetre en el país on realitzem la comunicació. És probable que el Punt d' Accés disposi d'un mètode automàtic el qual seleccioni la freqüència en funció del nivell de soroll que presenti un canal. Per exemple el primer canal lliure que trobi serà el que utilitzarà per la connexió. En cas de no trobar-ne cap de lliure, triarà el que menys interferències presenti.

3.2.2. Objectiu

Configurar les opcions bàsiques d'un Punt d' Accés per poder implementar una xarxa WiFi.

3.2.3. Realització

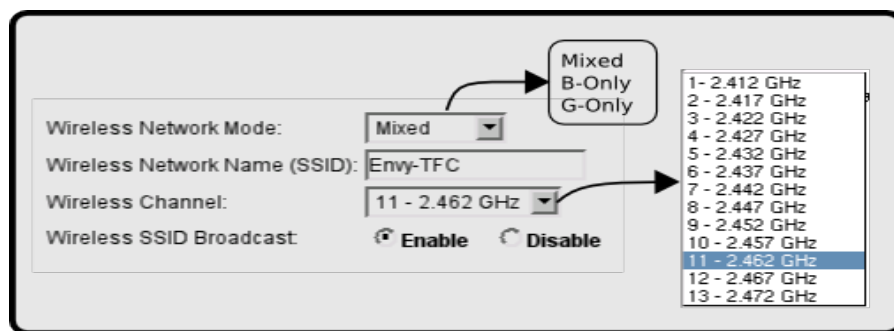
1. Connectem al Punt d' Accés mitjançant la interfície de xarxa ethernet.

Aquest és el mètode més aconsellable per l'administració segura del Punt d' Accés.

***Nota:** en cas de ser la primera configuració de l'aparell, és recomanable seguir les instruccions que el fabricant facilita amb el Punt d' Accés.*

2. Configurem el Punt d'Accés mitjançant web.

Per tant obrim un navegador i podem la adreça IP del Punt d' Accés. Quan ens paregui la pàgina de configuració, definim les opcions bàsiques:



Imatge 1. Opcions bàsiques d'un Punt d' Accés

Tipus de Xarxa: Ens defineix el protocol amb el qual treballarà el Punt d' Accés. En aquest cas permet treballar amb 802.11b i 802.11g. Podem forçar a la xarxa que treballi només amb un dels dos (els equips que es vulguin connectar hauran de treballar amb aquest protocol) o bé triar *Mixed* (el Punt d'accés permet treballar amb ambdós protocols). En aquest cas la xarxa intentarà que sempre es treballi amb G però només que un dels clients no el suporti, la xarxa canviarà automàticament a B.

- **Nom de la Xarxa (SSID):** Definim el nom de la xarxa, en el nostre cas posem “Envy-TFC”.

- **Canal:** Definim el canal 11 (freqüència 2.462 Ghz). Les comunicacions de la nostra xarxa aniran totes per aquest canal.

- **SSID Broadcast:** en aquí marquem que sí que volem que el Punt d' Accés emeti *Beacon Frames* amb el SSID de la xarxa per facilitar la connexió als usuaris.

3.3. Configuració del Client: Wireless Extensions – Wireless Tools

En aquesta segona pràctica configurarem un client en una xarxa *WiFi* a partir d'un conjunt d'eines anomenades *Wireless Tools*. Aquestes eines ens permeten controlar una sèrie de paràmetres de la interfície *WiFi* així com extreure'n informació d'estat mitjançant les *Wireless Extensions*.

3.3.1. Conceptes teòrics

Les *Wireless Extensions* és una API que permet manipular les interfícies de xarxa WiFi. Està composta per un conjunt de funcions i arxius de configuració els quals ens permeten obtenir informació en temps real de l'estat de la nostra interfície.

Les *Wireless Tools* són eines implementades a partir de les *Wireless Extensions* i ens serveixen per canviar la configuració d'aquesta interfície *on the fly*, obtenir l'actual configuració, estadístiques o bé analitzar-la.

Nosaltres en centrarem en les eines les quals ens ajudaran a entendre alguns conceptes teòrics bàsics del funcionament de les WLAN.

IWCONFIG és l'eina principal la qual ens permet obtenir dades i configurar la interfície de xarxa. Tot seguit podem veure algunes de les seves opcions.

```
iwconfig [interface]
        iwconfig interface [essid X] [nwid N] [mode M] [freq F]
                                [channel C] [sens S ] [ap A ] [nick NN ]
                                [rate R] [rts RT] [frag FT] [txpower T]
                                [enc E] [key K] [power P] [retry R]
                                [commit]
```

Consell: Per obtenir informació detallada del funcionament de **IWCONFIG** podem consultar les pàgines del manual de la nostra distribució. Obrim un terminal i teclegem `man iwconfig`.

INTERFACE: s'ha de substituir pel nom de la interfície *WiFi* que volem configurar. En funció del *driver* que utilitzem per controlar la targeta *WiFi* aquest utilitzarà un nom o un altre. Els més comuns en GNU/Linux són `eth1`, `wlan` o

ath0.

Consell: si obrim un terminal i teclegem *IWCONFIG* ens apareixerà un llistat de les interfícies WiFi disponibles.

ESSID: ens permet establir el nom de la xarxa a la que volem connectar.

MODE: ens permet canviar el mode dins la nostra xarxa. En funció del rol que assumim a la xarxa, el nostre mode pot ser:

- Si som Client:
 - Ad-Hoc:* ens permet crear un xarxa punt a punt, sense Punt d'Accés.
 - Managed:* ens permet connectar a una xarxa amb un o més Punts d'Accés.
- Si som Punt d'Accés:
 - Master:* ens habilita per ser Punt d'Accés.
 - Repeater:* ens permet fer forward de paquets entre diferents nodes.
 - Secondary:* ens permet actuar com a Punt d'Accés de backup.
- Només volem escoltar paquets:
 - Monitor:* ens permet posar la interfície escoltant el medi sense emetre cap paquet.

Nota: no totes les targetes WiFi suporten els modes *Master*, *Repeater*, *Secondary* i *Monitor*. També es pot provar d'actualitzar el firmware de la targeta.

3.3.2. Objectiu

Familiaritzar-nos amb algunes comandes sota GNU/Linux per connectar a una xarxa WiFi amb les opcions bàsiques.

3.3.3. Realització

1. Primer hem de localitzar la interfície *wireless* en el nostre equip.

```
Envy-Laptop # iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11g  ESSID:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s  Tx-Power:15 dBm  Sensitivity=0/3
          Retry:off  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-94 dBm  Noise level=-94 dBm
          Rx invalid nwid:160921  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Nota: tot i no ser recomanable per comoditat realitzarem totes les opcions com a Root.

Veiem que el sistema reconeix la interfície ath0 com a *wireless* i ens mostra l'estat dels paràmetres associats.

Podem veure que es tracte d'una interfície 802.11g i que d'entrada està configurada en *Mode Managed*. La resta de paràmetres semblen estar sense inicialitzar.

2. Associació a la xarxa.

Aprofitarem una de les opcions de l'eina IWCONFIG per associar-nos a la xarxa Envy-TFC.

```
Envy-Laptop # iwconfig ath0 essid "Envy-TFC"
```

3. Comprovem l'associació: IWCONFIG.

```
Envy-Laptop # iwconfig ath0  
  
ath0      IEEE 802.11g  ESSID:"Envy-TFC"  
Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70  
Bit Rate:54 Mb/s   Tx-Power:17 dBm   Sensitivity=0/3  
Retry:off   RTS thr:off   Fragment thr:off  
Encryption key:off  
Power Management:off  
Link Quality=71/94  Signal level=-27 dBm  Noise level=-95 dBm  
Rx invalid nwid:160929  Rx invalid crypt:0  Rx invalid frag:0  
Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

4. Configuració de la IP.

Per fer això utilitzarem les eines habituals de xarxa en GNU/Linux, la comanda IFCONFIG.

Sabem que el Punt d'Accés disposa d'una adreça 192.168.0.1/24, per tant hem de seleccionar una IP dins del mateix rang de xarxa.

```
Envy-Laptop# ifconfig ath0 192.168.0.10/24
```

I tot seguit fem PING al Punt d' Accés.

```
Envy-Laptop # ping -c3 192.168.0.1  
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.  
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=1.55 ms  
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=1.57 ms  
64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=1.57 ms
```

3.4. Paràmetres d'enllaç: Link Quality Anàlisi (LQA)

La qualitat de l'enllaç en una xarxa *WiFi* definirà en gran mesura les possibilitats d'ús i en determinarà el rendiment. Veurem com afecten les diferents modulacions a la transmissió d'informació i les possibles diferències entre canals. Anem a comprovar amb la següent pràctica com podem conèixer aquests paràmetres i com interpretar-los.

3.4.1. Conceptes teòrics

802.11 en Freqüència i Modulació

A l'any 1997, quan aparegueren 802.11a i 802.11b, es va poder comprovar com per xarxes amb visibilitat directa i llargues distàncies 802.11a es desenvolupa a 54 Mbps mentre que 802.11b ho fa a 11 Mbps. Però a curta distància i entorns de visibilitat reduïda és 802.11b el que millor treballa, ajustant la velocitat en funció de la qualitat de l'enllaç. Els motius es poden simplificar en 2 factors determinants:

- Freqüència (A: 5Ghz – B: 2.4 GHz)
- Modulació (A: OFDM – B: DSSS)

Referent a la freqüència podríem dir que a major freqüència major velocitat. Però en aquest cas no és estrictament l'únic factor que diferencia les velocitats de transmissió aconseguides per A i B. La liberalització de canals en la banda dels 5 Ghz va provocar alguns conflictes amb serveis de caire militar. Per aquest motiu l'any 2004 apareix 802.11h el qual intenta resoldre problemes derivats de la coexistència de les xarxes 802.11 amb sistemes de radars i satèl·lits a la banda dels 5 GHz (802.11a).

Per tal de respectar aquests requeriments, 802.11h proporciona a les xarxes 802.11a la capacitat de gestionar dinàmicament tant la freqüència, com la potència de transmissió. Ho fa mitjançant dues funcionalitats:

- *DFS (Dynamic Frequency Selection)*: evita interferències co-canal amb sistemes de radar i assegura una utilització uniforme dels canals disponibles.

- *TPC (Transmitter Power Control)*: assegura que es respecten les limitacions de potència transmesa que hi pot haver per diferents canals en una determinada regió de manera que es minimitza la interferència amb sistemes de satèl·lit.
-

Per això en comunicacions en temps real (VoIP, *streaming* d'àudio/vídeo) és preferible utilitzar la 802.11a, ja que la banda dels 5 Ghz sovint és més neta que la dels 2,4 Ghz.

Aquell mateix any apareix 802.11g el qual modula amb OFDM però a la banda dels 2.4 Ghz, obtenint velocitats de 54 Mbps també.

Es pot dir que 802.11g utilitza el millor d'ambdós protocols en el referent a transmissió. Ho podem veure en l'escalat de velocitat que realitza cadascun dels protocols en funció de la qualitat de senyal rebuda. És aquí quan 802.11g utilitza la seva polivalència alhora de modular. Ho podem comprovar en la següent taula:

Mbps	802.11a	802.11b	802.11g
54	OFDM	-	OFDM
48	OFDM	-	OFDM
36	OFDM	-	OFDM
24	OFDM	-	OFDM
18	OFDM	-	OFDM
12	OFDM	-	OFDM
11	-	DDDS (CCK)	DDDS (CCK)
9	OFDM	-	OFDM
6	OFDM	-	OFDM
5,5	-	DDDS (CCK)	DDDS (CCK)
2	-	DDDS (CCK)	DDDS (DBPSK/DQPSK)
1	-	DDDS (CCK)	DDDS (DBPSK/DQPSK)

Taula 2. Taula de Modulació en funció del bitrate i el protocol

OFDM (Orthogonal Frequency Division Multiplexing): modula la informació en moltes freqüències portadores amb poca taxa de símbols enlloc de modular en una sola freqüència amb una taxa elevada de símbols. Tenir una menor taxa de símbols per portadora es tradueix en un període de símbol més gran, el que proporciona protecció contra els ecos produïts pels múltiples camins que pren el senyal en la seva propagació. Aquest cas es dona

freqüentment a espais tancats o de poca visibilitat, on es pot rebre un senyal directe del transmissor més una certa quantitat de senyals retardats per les reflexions amb els edificis.

El fet de tenir un gran nombre de portadores on es distribueix la informació proporciona una protecció contra interferències co-canal, ja que si es perd la informació d'una portadora degut a aquestes interferències, es perd una petita part de la informació que no té perquè ser rellevant per a la qualitat de la transmissió. El senyal modulats té una banda de guarda, que és un període de temps on el senyal es manté constant durant un temps, repetint el símbol. D'aquesta forma els senyals que arriben amb un retard menor que el temps de banda de guarda es poden aprofitar com a senyals constructius per millorar la recepció.

DDDS (Direct-Sequence Spread Spectrum): en aquest procés la senyal modulada pren més ample de banda que la senyal original amb la informació. D'aquí el nom de *Spread Spectrum*: la senyal portadora està per sobre del màxim ample de banda del senyal a transmetre. La variant CCK (*Complementary Key Keying*) transmet les dades en símbols de 8 blocs DDDS, on cadascun d'ells és un parell de bits complex en QPSK a velocitats de 11 Mbps. Tot plegat fa que hi hagi una sobre-ocupació de l'espai radioelèctric a la banda dels 2.4 Ghz degut a la modulació escollida en B i a l'aparició massiva de dispositius en aquesta banda.

A partir de la taula anterior podem observar que A i G es comporten millor en espais oberts i de bona visibilitat, però quan aquesta és reduïda baixa radicalment la velocitat. És quan G adopta la modulació de B i permet la comunicació tot i que a menor velocitat que l'especificació original. Comparant A i B, veiem que quan el nivell de senyal és baix, B és capaç de regular més eficientment la velocitat. En canvi amb A aconseguim velocitats que B no suporta. G el que fa és modular amb OFDM els nivells amb bona qualitat de senyal. Quan arriba als 11 Mbps passa a modular igual que B

menys en entorns de poca qualitat de senyal.

Opcions i informació de IWCONFIG

Continuarem amb les opcions de IWCONFIG, en aquest cas referents a valors de la transmissió i del medi.

```
iwconfig [interface]
        iwconfig interface [essid X] [nwid N] [mode M] [freq F]
                                [channel C] [sens S ] [ap A ] [nick NN ]
                                [rate R] [rts RT] [frag FT] [txpower T]
                                [enc E] [key K] [power P] [retry R]
                                [commit]
```

TXPOWER: Ens permet determinar la potència de transmissió pels paquets de dades. Els valors que introduïm sense unitats seran interpretats com a dBm però podem especificar les unitats com mW. Per defecte treballa en mode AUTO.

FRAG: Podem fixar la mida màxima de fragmentació dels paquets en bytes.

A més teclejant només la comanda IWCONFIG [interface] la sortida ens mostra diferents paràmetres també interessants, el valor dels quals dependrà absolutament del *Driver* i del *Chipset* de la targeta *WiFi*.

Link quality: mesura la qualitat de l'enllaç en termes generals. Es pot interpretar com la relació de paquets que s'envien i els que es reben.

Per exemple: *Link Quality= 50/94 podem establir que si s'envien 94 paquets, 50 seran els que arribaran a destí (els altres colisionaran o es perdran pel medi).*

Nota: *per pròpia definició del protocol, mai obtindrem el 100% en les transmissions. Per això es pren el valor màxim com a 94 i no 100.*

Ha de basar-se en el nivell de contenció i interferència, la probabilitat d'error de bit, la qualitat de la senyal rebuda, temps de sincronització i altres mesures pròpies del *hardware*. Tot plegat fa que el valor final vari en funció del *Driver* i el *Chipset* de la targeta. S'ha de notar que el valor final és una probabilitat, no és un valor absolut.

- Signal level: és la potència de senyal rebuda, acostuma a presentar-se en dBm.
- Noise level: indica el nivell de soroll del medi (mesurat quan no es rep o transmet cap paquet)
- Rx invalid nwid: Nombre de paquets rebuts amb NWID o SSID diferent. Pot ajudar-nos a detectar errors en la configuració o indicar que algú altre està emetent en la mateixa freqüència.
- Missed beacon: Nombre de *Beacons Frames* que no s'han rebut del Punt d' Accés o node. Els *Beacon Frames* s'envien de forma periòdica de manera que si en l' interval esperat no hem rebut la notificació, Missed beacon s'incrementa en 1. Habitualment aquest fet ens indica que estem fora de la zona de cobertura de la xarxa.

I finalitzarem aquest apartat amb IWLIST, una comanda que ens permet saber més informació. En aquest cas els valors possibles dels camps de IWCONFIG.

IWLIST

- *[interface] scanning*: ens fa un *scan* del medi indicant possibles connexions.
- *[interface] frequency, channel*: ens llista els canals i freqüències disponibles per a la nostra interfície.
- *[interface] bitrate, rate*: llista les diferents velocitats que la interfície pot treballar.
- *[interface] encryption, key*: ens mostra la relació de claus i mètodes d' encriptació que disposa la interfície
- *[interface] power*: mostra les opcions de directives possibles del Punt d' Accés que la interfície pot suportar.
- *[interface] txpower*: llista les diferents potències d'emissió en que la interfície pot treballar
- *[interface] retry*: mostra si hi ha límit establert alhora de mantenir una connexió.
- *[interface] ap, accesspoints, peers*: llista les connexions disponibles.
- *[interface] event*: mostra els codis en hexadecimal de les

interrupcions per establir cadascuna de les opcions en la interfície.

3.4.2. Objectiu

Entendre i interpretar la informació que ens mostra la interfície *wireless* així com identificar la informació referent a la qualitat de l'enllaç. Veure la relació entre els diferents paràmetres, identificar el millor canal per emetre i poder delimitar zones de cobertura amb la informació de la targeta. Veure diferències entre les bandes de freqüència i els protocols.

3.4.3. Realització

1. Configuració de la xarxa.

Veure exercici 1-2.

3. Realització de mesures.

Canviem paràmetres físics (distància, zones de visibilitat) i paràmetres dels equips (potència, canals) per veure com afecten al funcionament de la xarxa.

4. Situació inicial: Ubiquem el client i el Punt d'Accés en una mateixa habitació amb visibilitat directa.

En el client teclegem IWCONFIG i veiem la informació que ens dóna.

```
Envy-Laptop # iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"
    Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70
    Bit Rate: 54 Mb/s   Tx-Power=15 dBm   Sensitivity=0/3
    Retry:off   RTS thr:off   Fragment thr:off
    Encryption key:off
    Power Management:off
    Link Quality=88/94  Signal level=-37 dBm  Noise level=-96 dBm
    Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
    Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Link Quality: 88%

Veiem també que la velocitat és de 54 Mb/s, el nivell de senyal - 37 dBm i el de soroll a -96 dBm. Els comptadors els tenim tots iniciats a 0.

Situació 2: Ubiquem el client en una altre habitació, sense visibilitat directa i teclegem IWCONFIG

```
Envy-Laptop # iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70
          Bit Rate:36 Mb/s   Tx-Power=15 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=28/94  Signal level=-68 dBm  Noise level=-96 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Link Quality: 28 %

El nivell de senyal a passat de -37 a -68 i la velocitat de 54 Mb/s s'ha ajustat automàticament a 36 Mb/s. En aquí podem veure com en funció del nivell de senyal obtingut, el Punt d'Accés regula la velocitat de transmissió.

Amb IWLIST podem veure l'escalat de velocitats que pot realitzar el nostre equip:

```

Envy-Laptop fede # iwlist ath0 bitrate
ath0      12 available bit-rates :
           1 Mb/s
           2 Mb/s
           5.5 Mb/s
           6 Mb/s
           9 Mb/s
          11 Mb/s
          12 Mb/s
          18 Mb/s
          24 Mb/s
          36 Mb/s
          48 Mb/s
          54 Mb/s
           Current Bit Rate:36 Mb/s

```

5. Cerquem el llinar de cobertura de la nostra xarxa.

Per fer-ho ens allunyarem fins que el camp *missed beacon* comenci a marcar *Beacon Frames* perduts.

```

Envy-Laptop# iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70
          Bit Rate:1 Mb/s   Tx-Power=off    Sensitivity=0/3
          Retry:off   RTS thr:off    Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=1/94  Signal level=-88 dBm  Noise level=-96 dBm
          Rx invalid nwid:145  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:2

```

Link Quality: 1%.

Veiem que el nivel de senyal és molt baix, -88 dBm i que el Bit Rate ha baixat al mínim és a dir, 1 Mbps. Amb aquests paràmetres hem

començat a no rebre Beacon Frames en els temps prevists i el comptador en marca 2 de no rebuts.

En el punt on hem obtingut aquests resultats podríem establir que és el punt límit de cobertura de la nostra xarxa (pel nivell de senyal i el *Link Quality*).

Clar que també s'ha de tenir en compte que pot ser un “punt negre” on no arriba senyal tot i estar dins de la zona de cobertura teòrica. Això pot ser degut a rebots, interferències, absorcions de senyal...

El camp *Rx invalid nwid* ha detectat fins ara 145 paquets que no són de la nostra xarxa. Això indica que hi ha una o més xarxes emetent en el mateix canal que nosaltres o bé en algun canal solapat.

Tots aquests factors s'han de tenir en compte per administrar correctament la xarxa. Per saber a què és degut aquest baix *Link Quality* primer hauríem de buscar un canal lliure, el màxim allunyat possible dels altres, i realitzar de nou les mesures en la mateixa zona.

6. Detectem si tenim xarxes al voltant i quins canals ocupen.

```
Envy-Laptop fede # iwlist ath0 scanning
ath0      Scan completed :
          Cell 01 - Address: 00:11:95:9C:90:CC
                  ESSID:"Xarxa-1"
                  Mode:Master
                  Frequency:2.437 GHz (Channel 6)
                  Quality=18/94  Signal level=-77 dBm  Noise level=-95 dBm
                  Encryption key:on
                  Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 22 Mb/s
                           6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                           36 Mb/s; 48 Mb/s; 54 Mb/s
                  Extra:bcn_int=200
          Cell 02 - Address: 00:18:39:28:3A:70
                  ESSID:"Envy-TFC"
                  Mode:Master
                  Frequency:2.462 GHz (Channel 11)
                  Quality=65/94  Signal level=-30 dBm  Noise level=-95 dBm
                  Encryption key:off
                  Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 22 Mb/s
                           6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                           36 Mb/s; 48 Mb/s; 54 Mb/s
                  Extra:bcn_int=100
          Cell 03 - Address: 00:11:50:F9:58:B0
                  ESSID:"Xarxa-2"
                  Mode:Master
                  Frequency:2.462 GHz (Channel 11)
                  Quality=7/94  Signal level=-88 dBm  Noise level=-95 dBm
                  Encryption key:on
                  Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s
                  Extra:bcn_int=100
                  IE: IEEE 802.11i/WPA2 Version 1
                     Group Cipher : CCMP
                     Pairwise Ciphers (1) : CCMP
                     Authentication Suites (1) : PSK
```

Podem veure que hi ha un total de 2 xarxes més:

- *Xarxa_1*: Emet pel canal 6, disposa de seguretat (probablement WEP), és una xarxa de Punt d' Accés i la qualitat de l'enllaç amb nosaltres és del 18%.
- *Xarxa_2*: emet pel canal 11, disposa de seguretat (WPA2), és

una xarxa de Punt d' Accés i la qualitat de l'enllaç és d'un 7%.

D'aquesta informació el més rellevant per nosaltres és que la *Xarxa_2* està en el mateix canal que nosaltres. La poca qualitat d'enllaç indica que està allunyada però al no ser 0 vol dir que ens arriben paquets aliens, així ho indica el comptador *RX invalid nwid*.

```
Envy-Laptop# iwconfig ath0
...
Rx invalid nwid:1450 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Veiem que el comptador s'ha incrementat fins a 1450. En funció del tràfic de l' altre xarxa el comptador s' incrementarà més ràpidament.

***Nota:** si tenim una altra xarxa emetent en el mateix canal que nosaltres, el més recomanable és canviar el nostre. Lo ideal és buscar la màxima separació possible sempre que la banda ho permeti. (ex: Si algú està al canal 6, el 1 i el 11 són la millor opció).*

3.5. Modes de connexió: *Ad-Hoc* i Infraestructura.

En funció de les nostres necessitats, la tecnologia *WiFi* proposa diferents tipus d'estructures alhora d'implementar una xarxa. En aquest exercici veurem les dues més significatives: *Ad-Hoc* i Infraestructura. Veurem el seu funcionament i les seves característiques.

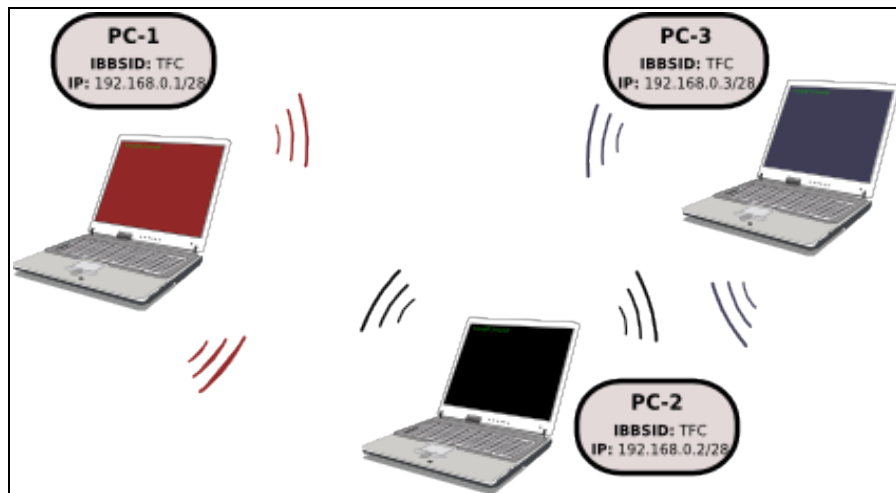
3.5.1. Conceptes teòrics

Dins la terminologia *WiFi* trobem constantment se'ns fa referència a la denominació Node. Un node es refereix a un punt de connexió, la unitat bàsica en una xarxa *WiFi*. El podem definir com a qualsevol aparell amb interfície *wireless*, que es pugui comunicar per aquest mitjà. Per tant una PDA, un ordinador portàtil, un PC, un Punt d'Accés, un *Bridge*...qualsevol d'aquest aparells si disposa d'interfície *wireless* pot ser un node de la nostra xarxa.

En funció dels nostres requeriments la tecnologia *WiFi* disposa de dos modes de connexió alhora d'implementar una xarxa: *Ad-Hoc* (basat en *Independent Basic Service Set*) i Infraestructura (Infraestructura/*Extended Basic Service Set*).

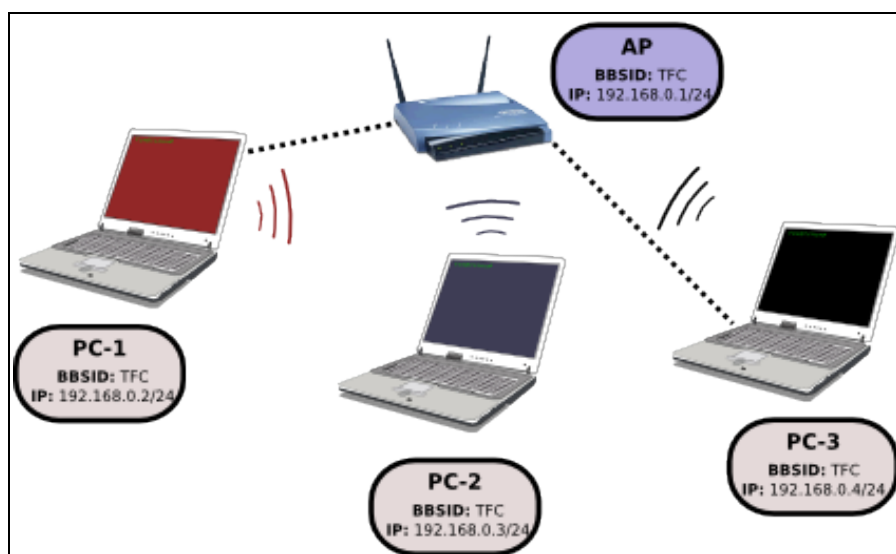
- ***Ad-Hoc***: es refereix a una mode de connexió punt a punt entre dos o més nodes. La informació d'un node es transmet a tots els nodes que estiguin en la mateixa xarxa, de manera que tots els nodes reben i envien els paquets de la xarxa. Aquest fa que a mida que incrementem els nodes, la informació enviada es va repetint creant molt de soroll en el medi. Aquest tipus de connexió pot ser útil per intercanviar de forma puntual informació entre dos o més aparells, però es fa insostenible per a xarxes amb densitat de tràfic i llarga durada. Per exemple si que pot ser habitual trobar xarxes on els seus nodes principals intercanvien informació de xarxa mitjançant connexió *Ad-Hoc* com és el cas de xarxes *MANets* (*Mobile Ad-Hoc Networks*) o les xarxes *Mesh*. A més

trobem més d'una cinquantena de protocols basats en aquesta topologia, normalment per comunicar Nodes.



Imatge 2. Xarxa Ad-Hoc

- **Infraestructura:** en aquest mode de connexió un dels nodes realitza la funció de node d'enllaç pel qual passen totes les connexions. A diferència del mode *Ad-Hoc*, només el node d'enllaç re-envia la informació. En el gràfic podem observar com per una comunicació entre el PC-1 i el PC-3 passa entremig del Punt d'Accés.



Imatge 3. Xarxa en mode Infraestructura

Segons les característiques del Punt d' Accés, aquest el podem configurar com a *Router* (de manera que doni accés a una altre xarxa), pot funcionar com a *Bridge* (pont entre dues xarxes) o de repetidor (estenenent l'àrea de cobertura).

3.5.2. Objectiu

Configurar una xarxa *Ad-Hoc* entre dos Clients.

3.5.3. Realització

1. Configurem 2 connexions Ad-hoc.

```
Equip-A # iwconfig ath1 mode ad-hoc && iwconfig ath1 essid Envy-TFC && ifconfig  
ath1 192.168.1.1/28 && iwconfig ath1 ap 0A:16:CB:BB:FF:B2  
  
Equip-B # iwconfig ath1 mode ad-hoc && iwconfig ath1 essid Envy-TFC && ifconfig  
ath1 192.168.1.2/28 && iwconfig ath1 ap 06:16:CB:BB:FF:A4
```

En una sola línia de codi (concatenant les comandes), podem establir el Mode, SSID, IP i el Punt d' Accés.

Nota: no totes les targetes suporten el mode Ad-Hoc. En funció de la targeta, canviar el Mode ens pot donar error.

2. Fem Ping.

```
Equip-A # ping -c3 192.168.1.3  
  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.039 ms  
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.035 ms  
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.035 ms  
  
--- 192.168.1.2 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.035/0.036/0.039/0.005 ms
```

Veiem que els equips estan en xarxa i que es comuniquen perfectament.

Capítol IV: Paràmetres de Seguretat.

4.1. Seguretat elemental: CNAC i ACL

No totes les xarxes requereixen un nivell de seguretat alt. En aquest apartat veurem les opcions més elementals per poder obtenir un mínim nivell de control sobre qui pot accedir a la nostra xarxa.

4.1.1. Conceptes teòrics

Referent a la seguretat, la primera proposta de 802.11b esdevé en controlar qui pot accedir a la xarxa. Per fer-ho utilitza dues tècniques que treballen a diferent nivell: una procura no fer visible a tothom la xarxa i l'altre es basa en restringir els equips que hi poden accedir.

- **CNAC (Closed Network Access Control):** mitjançant aquest mecanisme es pretén restringir la connexió als usuaris que coneixen prèviament el SSID de la xarxa. Per fer-ho no s'emeten els *Beacon Frames* que anuncien la xarxa, de manera que el SSID es converteix en una mena de clau d'accés.

Nota: Més endavant demostrarem perquè el SSID no s'ha d'entendre com una clau d'accés.

Aquesta tècnica es profitosa ja que no s'anuncia la ubicació ni el nom de la xarxa, fent-la inexistent a primer cop d'ull. Per contra força a qui es vol connectar a conèixer el nom de la xarxa.

- **ACL (Access Control List):** aquest mecanisme consisteix en una llista d'accés emmagatzemada en el Punt d'Accés la qual disposa de les adreces MAC dels dispositius que poden connectar a la xarxa. Si l'adreça física del client no apareix a la llista, aquest no es pot associar.

Aquesta tècnica permet a l'administrador a tenir un control més precís sobre quins equips es poden connectar a la xarxa. Per contra obliga a l'usuari a registrar, prèvia connexió, el seu equip.

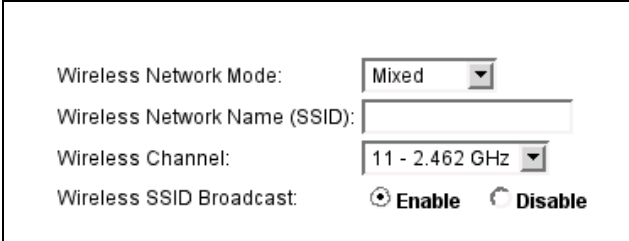
4.1.2. Objectiu

Configurar diferents opcions en una xarxa amb *Beacon Frames* i ACL, provant les diferents opcions i veure diferències.

4.1.3. Realització

1. Posem el SSID en blanc.

En aquest cas haurem d'introduir un espai en blanc ja que per defecte el Punt d'Accés no ens ho permet.



Wireless Network Mode: Mixed

Wireless Network Name (SSID):

Wireless Channel: 11 - 2.462 GHz

Wireless SSID Broadcast: ☒ Enable ☐ Disable

Imatge 4. Configuració del SSID Broadcast (Beacon Frames) en el Punt d'Accés

Realitzem un *Scan* per veure si apareix el Punt d'Accés

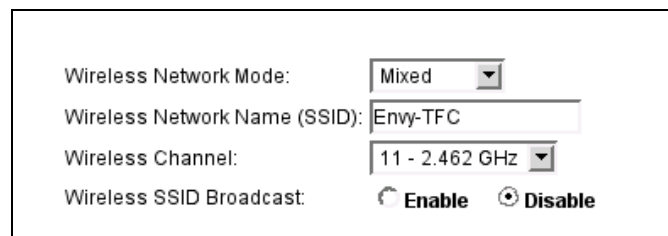
```
Envy-Laptop / # iwlist ath0 scan

ath0                               Scan      completed      :
Cell 01 - Address: 00:18:39:28:3A:70
    ESSID:" "
    Mode:Master
    Frequency:2.462 GHz (Channel 11)
    Quality=75/94  Signal level=-20 dBm  Noise level=-95 dBm
    Encryption key:off
    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 22 Mb/s
               6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
               36 Mb/s; 48 Mb/s; 54 Mb/s
    Extra:bcn_int=100
```

Veiem que apareix però amb el camp SSID amb un espai en blanc. En el moment d'omplir el camp del Punt d'Accés aquest no ens ha permès deixar en blanc el camp SSID.

2. Configurem el Punt d' Accés perquè no emeti Beacon Frames.

Marquem la opció *Disabled* en el *Wireless SSID Broadcast*



The image shows a configuration window for a wireless network. It contains four settings:

- Wireless Network Mode: Mixed (dropdown menu)
- Wireless Network Name (SSID): Envy-TFC (text input field)
- Wireless Channel: 11 - 2.462 GHz (dropdown menu)
- Wireless SSID Broadcast: ☒ Enable ☐ Disable (radio buttons)

Imatge 5. Deshabilitem els Beacon Frames

Fem un IWLIST ATH0 SCAN i veiem que no apareix cap resultat. Ara el que farem és posar-nos directament el SSID, en aquest cas Envy-TFC, i realitzem de nou un *scan*.

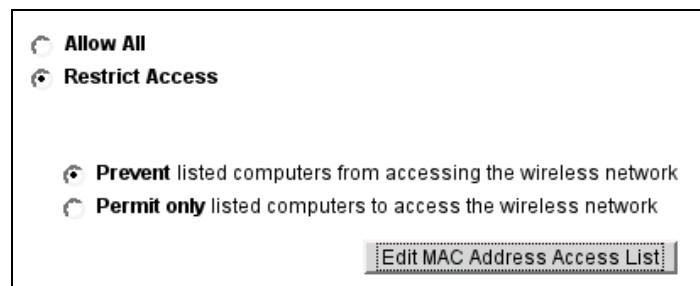
```
Envy-Laptop # iwconfig ath0 essid "Envy-TFC"

Envy-Laptop # iwlist ath0 scan
ath0      Scan completed :
    Cell 01 - Address: 00:18:39:28:3A:70
               ESSID: ""
               Mode:Master
               Frequency:2.462 GHz (Channel 11)
               Quality=75/94  Signal level=-20 dBm  Noise level=-95 dBm
               Encryption key:off
               Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 22 Mb/s
                           6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                           36 Mb/s; 48 Mb/s; 54 Mb/s
               Extra:bcn_int=100
```

Veiem que si podem detectar el Punt d' Accés (ho sabem per la MAC), però no apareix el SSID. Això és degut a que el client sap que hi és el Punt d'Accés, de fet hi està associat, però en cap moment aquest ha publicat el nom de la xarxa.

3. Configurem el Punt d' Accés perquè no accepti clients amb una MAC determinada.

Primer seleccionem la opció de bloquejar l'accés només als clients llistats a partir de la MAC del dispositiu.



Imatge 6. Opcions de restriccions ACL en el Punt d'Accés

Després posarem l'adreça MAC del client que volem excloure.

MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxxxx/xx:xx:xx:xx:xx:xx

MAC 01: 00:16:CB:BB:FF:B2	MAC 11:
MAC 02:	MAC 12:
MAC 03:	MAC 13:
MAC 04:	MAC 14:
MAC 05:	MAC 15:
MAC 06:	MAC 16:
MAC 07:	MAC 17:
MAC 08:	MAC 18:
MAC 09:	MAC 19:
MAC 10:	MAC 20:

Wireless Client MAC List

Imatge 7. Llistat d'adreces MAC a filtrar.

Llavors intentem associar-nos a la xarxa Envy-TFC

```

Envy-Laptop / # iwconfig ath0 essid Envy-TFC && iwconfig ath0 ap
00:18:39:28:3A:70
Envy-Laptop / # iwconfig ath0
ath0 IEEE 802.11a ESSID:"Envy-TFC"
        Mode:Managed Frequency:5.68 GHz Access Point: not-associated
        Bit Rate:0 Mb/s Tx-Power:15 dBm Sensitivity=0/3
        Retry:off RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=0/94 Signal level=-95 dBm Noise level=-95 dBm
        Rx invalid nwid:1323 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:0 Missed beacon:0

```

Veiem que no es produeix l' associació ja que el camp *Access Point* ens diu *not-associated*.

El llistat que hem definit en el Punt d'Accés era només per filtrar les adreces MAC que no poden connectar-se, per tant anem a provar que passa si canviem la MAC.

```
Envy-Laptop / # ifconfig ath0 down && ifconfig ath0 hw ether 00:12:33:25:4A:18
Envy-Laptop / # iwconfig ath0
ath0      Link encap:Ethernet HWaddr 00:12:33:25:4A:18
...
```

Per canviar-la primer hem de “baixar” la interfície, canviem la MAC i fem un IFCONFIG er veure que els canvis s'han realitzat correctament.

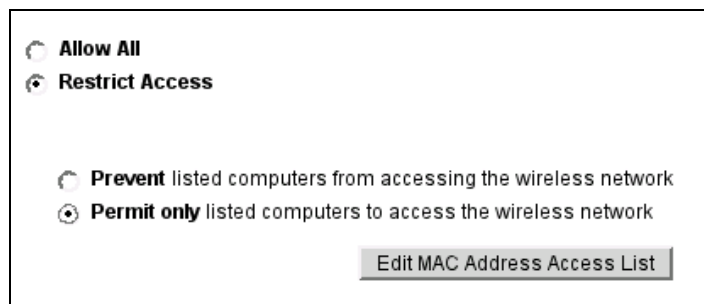
Tot seguit el que farem és “aixecar” de nou la interfície. Si tot va bé, com que ja tenim configurat el SSID, automàticament el client intenta associar-se a la xarxa i en principi no hauria de trobar la restricció per MAC ja que la hem canviada.

Executem altre cop IWCONFIG per veure que ha passat:

```
Envy-Laptop / # ifconfig ath0 up && iwconfig ath0
ath0      IEEE 802.11g ESSID:"Envy-TFC"
Mode:Managed Frequency:2.462 GHz Access Point: 00:18:39:28:3A:70
Bit Rate:54 Mb/s Tx-Power:15 dBm Sensitivity=0/3
Retry:off RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=75/94 Signal level=-66 dBm Noise level=-96 dBm
Rx invalid nwid:1543 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Veiem que ens hem pogut associar només canviant-nos l'adreça MAC. Sembla doncs que no és una forta mesura de seguretat.

4. Configurem el Punt d' Accés perquè només accepti clients amb una MAC determinada.

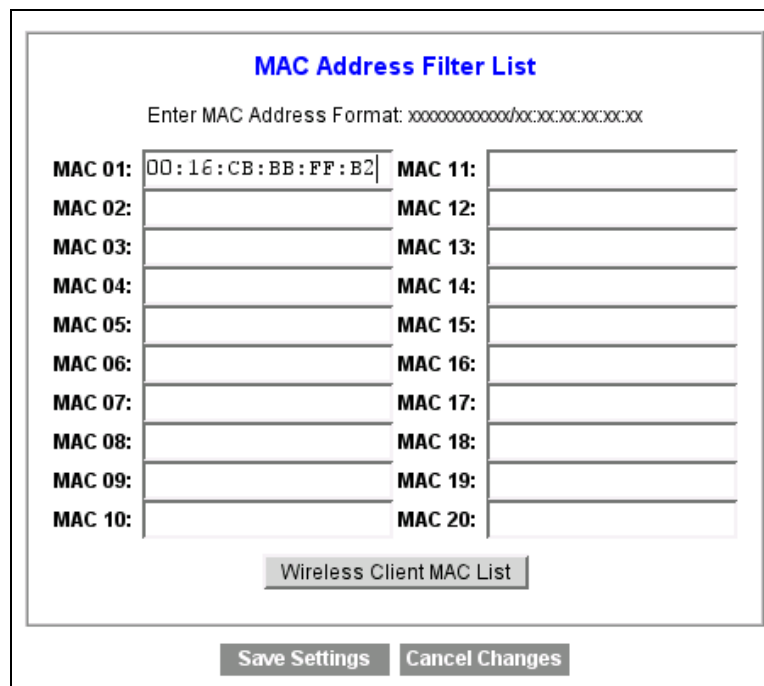


☐ Allow All
☒ Restrict Access

☐ Prevent listed computers from accessing the wireless network
☒ Permit only listed computers to access the wireless network

[Edit MAC Address Access List](#)

Imatge 8. Opcions de restriccions ACL en el Punt d'Accés Permit-Only



MAC Address Filter List

Enter MAC Address Format: xxxxxxxxxxxxxxxx:xx:xx:xx:xx:xx

MAC 01:	00:16:CB:BB:FF:B2	MAC 11:	
MAC 02:		MAC 12:	
MAC 03:		MAC 13:	
MAC 04:		MAC 14:	
MAC 05:		MAC 15:	
MAC 06:		MAC 16:	
MAC 07:		MAC 17:	
MAC 08:		MAC 18:	
MAC 09:		MAC 19:	
MAC 10:		MAC 20:	

[Wireless Client MAC List](#)

[Save Settings](#) [Cancel Changes](#)

Imatge 9. Llistat d'adreces MAC a filtrar

Com que disposem de la MAC canviada per l'exercici anterior, el Punt d' Accés no ens deixa associar-nos a la xarxa.

Nota: ho podem veure perquè el camp Access Point indica Not-Associated

El que farem és restablir l'adreça MAC i veure si el Punt d'Accés ens permet

l'Associació.

```
Envy-Laptop / # ifconfig ath0 down && ifconfig ath0 hw ether 00:16:CB:BB:FF:B2
Envy-Laptop / # ifconfig ath0
ath0 IEEE 802.11g ESSID:"Envy-TFC"

Mode:Managed Frequency:2.462 GHz Access Point: 00:18:39:28:3A:70
Bit Rate:54 Mb/s Tx-Power:15 dBm Sensitivity=0/3
Retry:off RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=74/94 Signal level=-67 dBm Noise level=-96 dBm
Rx invalid nwid:1701 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Podem veure com aquest cop si que ens ha permès l'associació ja que la MAC del Punt d' Accés apareix amb amb IWCONFIG.

4.2. Encriptació de Dades: WEP

Un dels apartats que pren més importància alhora de seguritzar les comunicacions sense fils és l'encriptació de les dades. A diferència de les xarxes *ethernet*, en *WiFi* la informació viatja per l'aire de manera que no es necessita estar físicament connectat al segment de xarxa per escoltar que s'està enviant. Per aquest motiu neix WEP i en els següents apartats veurem com funciona i com podem implementar-lo en una xarxa *WiFi*.

4.2.1. Conceptes teòrics

WEP (Wired Equivalent Privacy): és un sistema de xifrat que neix al l'any 1999 i s'incorpora al 802.11b amb l'objectiu de proveir a les connexions sense fils un grau equivalent de privacitat que les cablejades. Està basat en un algorisme de xifrat RC4 i utilitza claus de 64 bits (40 bits + 24 bits del Vector d'inicialització IV) o de 128 bits (104 bits + 24 bits del IV).

En necessiten tres eines pel xifrat de la informació: algorisme de xifrat RC4 (per xifrar la informació), un algorisme que valida la integritat del missatge basat en CRC (Control de Redundància Cíclica) i una clau. Aquesta clau es pot generar de dues maneres:

- **Introduint una “Frase de Pas”:** pot ser una paraula o frase fàcil de recordar a partir de la qual, aplicant una operació matemàtica, generarà 4 claus hexadecimal.
- **Introduint la clau directament:** haurà de ser de 40 o 104 bits, en funció de l'encriptat que vulguem realitzar, i serà en hexadecimal.

Per realitzar el procés d'encriptació WEP només utilitzarà una d'aquestes claus.

Procés d'encriptació.

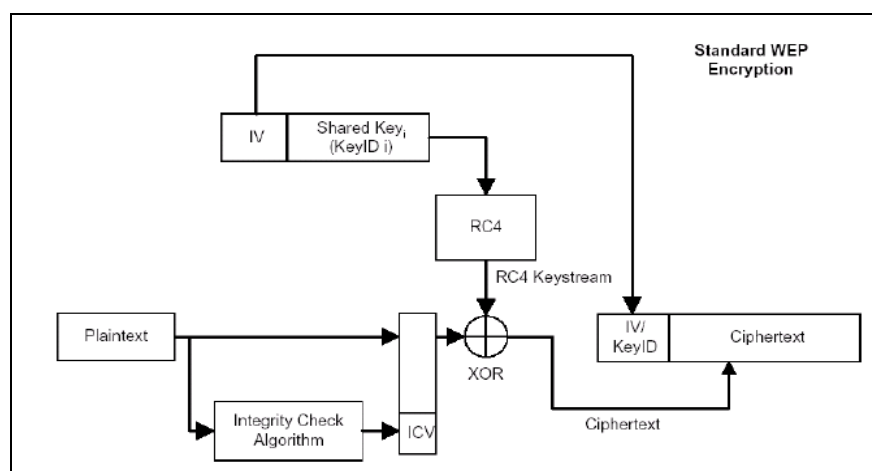
1. Apliquem l'algorisme CRC a la informació que volem enviar. Com a

resultat ens donarà un valor anomenat Vector de Control d' Integritat (ICV en anglès).

2. Per altre cantó a la clau triada li afegim un comptador de 24 bits (IV). I li apliquem l'algorisme de RC4

3. Realitzem un XOR del pas 1 i 2: el resultat serà:

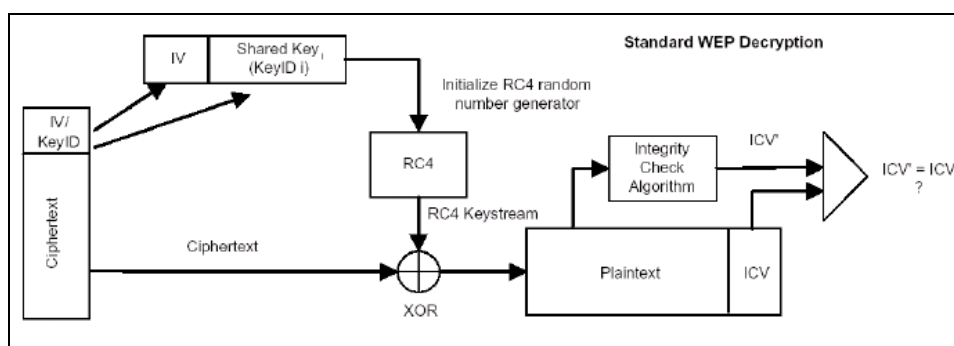
- La capçalera 802.11 + IV i el número de clau triada. Sense encriptar
- La informació + ICV. Encriptat.



Imatge 10. Encriptació WEP

Procés de desenscriptació.

1. A la clau triada li afegim el IV i apliquem l'algorisme de RC4.
2. Realitzem una XOR del (IV, Clau) i (Informació, ICV).
3. Apliquem l' algorisme de CRC a la informació i si coincideix amb el ICV rebut el resultat és correcte.



Imatge 11. Desenscriptació WEP

4.2.2. Objectiu

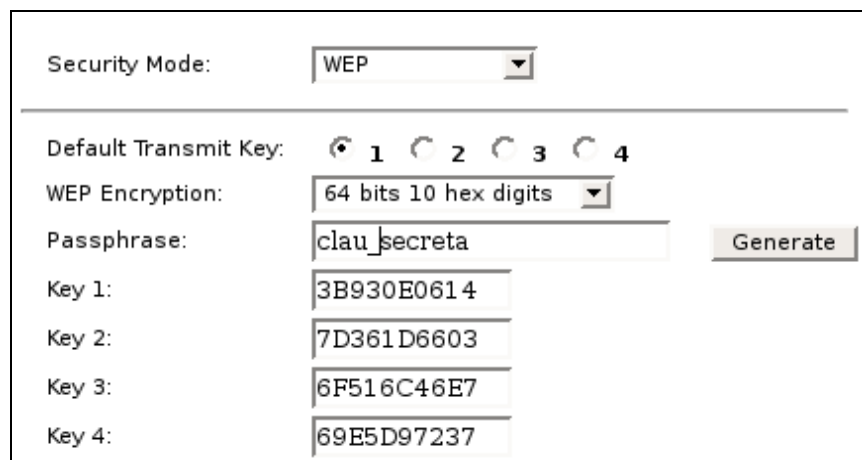
Configurar un Punt d' Accés amb encriptació web de 64 i 128 bits.

Veure si hi ha diferències en la transmissió amb la informació no encriptada, informació encriptada a 64 bits i informació encriptada a 128 bits.

4.2.3. Realització

1. Configurem el Punt d' Accés amb Encriptació WEP a 64 bits

- Configurem els paràmetres inicials de xarxa (veure Capítol 3)
- Seleccionem WEP/ 64 bits
- Posem una clau de pas que ens sigui fàcil de memoritzar
- L' aplicació WEP del Punt d' Accés disposa de la funció de l'algorisme de generació de claus i ens genera 4 claus.
- Seleccionem la clau que volem utilitzar per l' encriptació.



The screenshot shows a configuration window for WEP. At the top, 'Security Mode' is set to 'WEP'. Below this, 'Default Transmit Key' has four radio buttons labeled 1, 2, 3, and 4, with button 1 selected. 'WEP Encryption' is set to '64 bits 10 hex digits'. A 'Passphrase' field contains the text 'clau secreta', and a 'Generate' button is to its right. Below the passphrase, four keys are displayed in separate input fields: 'Key 1' is '3B930E0614', 'Key 2' is '7D361D6603', 'Key 3' is '6F516C46E7', and 'Key 4' is '69E5D97237'.

Imatge 12. Configuració WEP-64 del Punt d' Accés

Veiem que el sistema ens ha generat 4 claus de 10 dígit hexadecimals de 64 bits de les quals hem seleccionat la primera clau. Aquesta es la clau que hem de donar als clients que vulguin connectar a la xarxa.

2. Configurem el client.

Ens ajudarem del paràmetre ENC seguit de la clau en hexadecimal.

```
Envy-Laptop / # iwconfig ath0 enc 3B930E0614
```

Veiem quina informació ens mostra IWCONFIG

```
Envy-Laptop # iwconfig ath0 essid Envy-TFC && ifconfig ath0 192.168.0.2 &&
iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"
  Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70
  Bit Rate:36 Mb/s   Tx-Power:15 dBm   Sensitivity=0/3
  Retry:off   RTS thr:off   Fragment thr:off
  Encryption key:3B93-0E06-14   Security mode:restricted
  Power Management:off
  Link Quality=64/94  Signal level=-52 dBm  Noise level=-95 dBm
  Rx invalid nwid:0  Rx invalid crypt:52  Rx invalid frag:0
  Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

El client ja el tenim associat (tal i com mostra el camp *Access Point*). Els camps rellevants per l'encriptació WEP són:

- *Encryption key*: on ens mostra la clau d'encriptació en hexadecimal.
- *Rx invalid crypt*: són els paquets de la xarxa que no hem sabut resoldre la desenciptació. *Nota*: Normalment aquest es produeixen abans d'introduir la clau WEP.

3. Configurem el punt d'Accés amb encriptació WEP de 128 bits.

- Configurem els paràmetres inicials de xarxa (veure Capítol 3)
- Seleccionem WEP/ 64 bits
- Posem una clau de pas que ens sigui fàcil de memoritzar
- L'aplicació WEP del Punt d'Accés disposa de la funció de l'algorisme

de generació de claus i ens genera 4 claus.

- Seleccionem la clau que volem utilitzar per l' encriptació.

Security Mode: WEP

Default Transmit Key: 1 2 3 4

WEP Encryption: 128 bits 26 hex digits

Passphrase: clau secreta Generate

Key 1: 361A9BBC5F99508464C5C937AB

Key 2: 6D14D97EC7983AE0D33DF4E30C

Key 3: EA879858D124B4B20A00EA83DE

Key 4: 4712E574311CE1A37280EE7FE4

Imatge 13. Configuració WEP-128 en el Punt d' Accés

4. Configurem el client.

Ens ajudarem del paràmetre ENC seguit de la clau en hexadecimal en 128 bits. Només amb la longitud de la clau, el sistema ja reconeix que es tracta de WEP-128 bits.

```
Envy-Laptop / #iwconfig ath0 enc 361A9BBC5F99508464C5C937AB && iwconfig ath0
ath0 IEEE 802.11g ESSID:"Envy-TFC"
Mode:Managed Frequency:2.462 GHz Access Point: 00:18:39:28:3A:70
Bit Rate:36 Mb/s Sensitivity:0/3
Retry limit:off RTS thr:off Fragment thr:off
Encryption key:361A-9BBC-5F99-5084-64C5-C937-AB Security mode:restricted
Power Management:off
Link Quality=62/92 Signal level=-67 dBm Noise level=-96 dBm
Rx invalid nwid:0 Rx invalid crypt:52 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Veiem que s'associa sense cap problema al Punt d'Accés. Tornem a notar els paquets detectats a *RX invalid crypt*, altre cop degut a definir primer el SSID i després la clau WEP.

4.3. Autenticació. Open System i Shared Key

En aquest apartat veurem quins dos mètodes implementa 802.11b per autenticar els clients, les característiques de cadascun, el funcionament i com implementar-los.

4.3.1. Conceptes teòrics

Quan un client desitja connectar a una xarxa *WiFi* ha de conèixer el SSID d'aquesta. El client enviarà un missatge *PROVE REQUEST* amb ell SSID de la xarxa de manera que el Punt d' Accés que la gestioni inici amb el client un procés d'associació.

El procés d'associació a una xarxa *WiFi* contempla 3 estats possibles:

1. No autenticat / No associat
2. Autenticat / No Associat
3. Autenticat / Associat

Per poder passar d'un estat a un altre, el client i el Punt d' Accés s'enviaran uns paquets anomenats *Management Frames* els quals inclouran informació sobre les peticions de canvi d'estat i la resposta. Si el client desitja ser associat primer s'haurà d'autenticar.

L'autenticació és un procés mitjançant el qual un valida l'autenticitat d'una informació. Aquest pot ser la identitat d'una persona o la certesa d'una fet. En el camp de les comunicacions el procés d'autenticar valida que realment l'emissor i el receptor són qui diuen ser. I per fer-ho s'acostuma a utilitzen mecanismes basats en alguna cosa coneguda, com per exemple una clau.

802.11b proposa 2 sistemes per realitzar el procés d'autenticació:

- **Open System Authentication:** és el protocol per defecte i el seu

funcionament és molt simple. Qualsevol que demana ser autenticat és automàticament autenticat. Per tant no ofereix cap mesura de control ni comprova la identitat del sol·licitant: valida a tot aquell qui ho demana.

- **Shared Key Authentication:** aquest protocol es basa en que el client i el Punt d' Accés han de compartir un clau la qual validarà el procés. Aquesta clau vindrà disposada per l' encriptació WEP la qual ha d'estar activa per poder utilitzar aquesta autenticació. Bàsicament funciona en 5 passes:

1. El Client sol·licita al Punt d'Accés autenticar-se
2. El Punt d'Accés envia un Text de desafiament al client.
3. El client utilitza la clau WEP per encriptar el text de desafiament i l'envia al Punt d' Accés.
4. El punt d' Accés descripta el text rebut amb la seva clau WEP. Si coincideix amb l'original enviat, voldrà dir que els dos disposen la mateixa clau.
5. El punt d'accés envia l' acceptació i el client pot associar-se a la xarxa.

En cas de no coincidir les claus el Punt d' Accés enviarà no autenticarà el client, de manera que quan arribi al tercer estat del procés d'associació, i envii un *ASSOCIATION REQUEST*, el Punt d' accés li retornarà la negativa continguda en un *ASSOCIATION RESPONSE*.

IWEVENT

És una altra eina de les *Wireless-Tools* la qual ens permet veure en temps reals quins events estan succeint a la xarxa *WiFi*. En aquest tipus de xarxa trobem 2 tipus d'events:

-*Específics de la nostra interfície:* freqüència, velocitat, Nodes...

-*Esdeveniments de la xarxa:* fan referència als estats en un procés de comunicació. Per exemple, si estem associats o no, en canviem el mode, si establim una clau, si fem un scan del medi...

IWEVENT ens pot ser molt útil per veure quines accions s'estan duent a terme en temps reals amb la nostra interfície de xarxa.

4.3.2. Objectiu

Configurar el Punt d' Accés amb *Open System* i *Shared Key*. Configurar el client i veure les diferències en el moment de l'associació entre un mètode i l'altre.

4.3.3. Realització

1. Configurem el Punt d'Accés seleccionant Shared-Key.

Normalment aquest bé configurat en mode automàtic com a *Open System*, per tant hem d'especificar que volem utilitzar *Shared-Key*.

Nota: per habilitar *Shared-Key* necessitem establir un clau WEP.

Authentication Type:	Shared-Key ▼	(Default: Auto)
Control TX Rate:	Auto ▼	(Default: Auto)
Beacon Interval:	100	(Default: 100, Milliseconds, Range: 1 - 65535)
DTIM Interval:	1	(Default: 1, Range: 1 - 255)
Fragmentation Threshold:	2346	(Default: 2346, Range: 256 ~ 4096)
RTS Threshold:	2347	(Default: 2347, Range: 0 ~ 4096)

Imatge 14. Opcions avançades del Punt d'Accés

2. Configurem el client amb Shared Key.

Realitzem les mateixes passes per establir una clau WEP.

Utilitzarem IWEVENT per veure les diferents accions que succeixen en la nostra interfície.

Obrirem primer una consola amb iwevent i en una altre configurarem la interfície.

Consola 1:

```
Envy-Laptop:~$ iwevent  
  
Waiting for Wireless Events from  
interfaces...
```

Consola 2:

```
Envy-Laptop# iwconfig ath0 enc 361A9BBC5F99508464C5C937AB && iwconfig ath0 essid  
Envy-TFC && iwconfig ath0  
  
ath0 IEEE 802.11g ESSID:"Envy-TFC" Nickname:""  
Mode:Managed Frequency:2.462 GHz Access Point: 00:18:39:28:3A:70  
Bit Rate:36 Mb/s Tx-Power:13 dBm Sensitivity=0/3  
Retry:off RTS thr:off Fragment thr:off  
Encryption key:361A-9BBC-5F99-5084-64C5-C937-AB Security mode:restric  
Power Management:off  
Link Quality=23/94 Signal level=-63 dBm Noise level=-86 dBm  
Rx invalid nwid:58 Rx invalid crypt:0 Rx invalid frag:0  
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Podem veure com s'ha establert la clau a *Encryption-Key* i que ja estem associats al Punt d'Accés. Veiem que està succeint en la Consola 1

Consola 1:

```
...  
17:26:48.596236 ath0 Set Encryption key:****-****-****-****-****-****-***  
17:26:48.597868 ath0 New Access Point/Cell address:Not-Associated  
17:26:48.597912 ath0 Set ESSID:"Envy-TFC"  
17:26:48.601250 ath0 New Access Point/Cell address:00:18:39:28:3A:70
```

Veiem que s'estableix la clau WEP, però el client no es pot associar perquè encara no sap a quin Punt d'Accés. Al establir el SSID el client sap a quina xarxa s'ha d'unir i per tant busca el Punt d'Accés d'aquella xarxa amb millor Qualitat d'enllaç. Com que en la nostra xarxa només en hi ha un, dons

prova d'associar-se en aquest i ho aconseguim.

3. Configurem el client amb *Shared Key* amb una clau WEP errònia.

Modifiquem la darrera B de la clau per una A.

```
Envy-Desktop:# iwconfig ath0 enc 361A9BBC5F99508464C5C937AA && iwconfig ath0
essid Envy-TFC && iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"  Nickname:""
          Mode:Managed  Frequency:2.462 GHz  Access Point: Not-Associated
          Bit Rate:36 Mb/s   Tx-Power:13 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key: 361A-9BBC-5F99-5084-64C5-C937-AA   Security
mode:restricted
          Power Management:off
          Link Quality=20/94  Signal level=-76 dBm  Noise level=-96 dBm
          Rx invalid nwid:7850  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon: 0
```

Veiem que ens diu la sortida de la Consola 1:

```
...
18:01:37.798395  ath0      Set Encryption key:****-****-****-****-****-****-***
18:01:37.799917  ath0      Set ESSID:"Envy-TFC"
18:01:44.796430  ath0      Scan request completed
18:01:51.824404  ath0      Scan request completed
18:01:58.824387  ath0      Scan request completed
18:02:05.852355  ath0      Scan request completed
18:02:12.852343  ath0      Scan request completed
18:02:19.880301  ath0      Scan request completed
18:02:20.791064  ath0      Set Mode:Managed
18:02:27.904280  ath0      Scan request completed
18:04:21.170686  ath0      Set Mode:Managed
18:04:28.307853  ath0      Scan request completed
...
```

A l'igual que abans s'estableix la clau WEP, el SSID i es realitza un *scan* per trobar el Punt d' Accés. Realitza fins a 6 *scans* en intervals de 7 segons cadascun i sembla ser que no troba la xarxa Envy-TFC.

4. Configurem el client amb autenticació *Open System* i encriptació WEP.

Modifiquem el Punt d'Accés a autenticació automàtica (*Open System*).

Configurem el client novament amb la clau errònia.

Consola 2:

```
Envy-Laptop:/# iwconfig ath0 enc 361A9BBC5F99508464C5C937AA && iwconfig ath0
essid Envy-TFC && iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"  Nickname:""
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70
          Bit Rate:48 Mb/s   Tx-Power:13 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
                  Encryption key:361A-9BBC-5F99-5084-64C5-C937-AA      Security
mode:restricted
          Power Management:off
          Link Quality=17/94  Signal level=-69 dBm  Noise level=-86 dBm
          Rx invalid nwid:12911  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Hem canviat la darrera B de la clau per una A. Malgrat tot sembla que el Client s'ha pogut associar. Anem-ho a comprovar veient que ha passat a la Consola 1.

Consola 1:

```
...
18:13:33.070275  ath0      Set Encryption key:****-****-****-****-****-****-**
18:13:33.071675  ath0      Set ESSID:"Envy-TFC"
18:13:40.194049  ath0      Scan request completed
18:13:40.199587  ath0      New Access Point/Cell address:00:18:39:28:3A:70
...
```

Veiem que efectivament el client està associat amb el Punt d'Accés. Per tant formar part de la xarxa tot hi disposar d'una clau

errònia.

Llavors anem a fer PING al Punt d' Accés.

```
Envy-Laptop:/# ifconfig ath0 192.168.1.21
Envy-Laptop:/# ping -c3 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.21 icmp_seq=1 Destination Host Unreachable
From 192.168.1.21 icmp_seq=2 Destination Host Unreachable
From 192.168.1.21 icmp_seq=3 Destination Host Unreachable

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2003ms
```

Sembla ser que no està en xarxa. El que farem ara es provar d'introduir la clau WEP vàlida i tornar a fer PING.

```
Envy-Laptop:/# iwconfig ath0 enc 361A9BBC5F99508464C5C937AB && iwconfig ath0
essid Envy-TFC && ifconfig ath0 192.168.1.21 && iwconfig ath0
ath0      IEEE 802.11g  ESSID:"Envy-TFC"  Nickname:""
Mode:Managed  Frequency:2.462 GHz  Access Point: 00:18:39:28:3A:70
Bit Rate:36 Mb/s   Tx-Power:13 dBm   Sensitivity=0/3
Retry:off   RTS thr:off   Fragment thr:off
Encryption key:361A-9BBC-5F99-5084-64C5-C937-AB   Security mode:rest
Power Management:off
Link Quality=20/94  Signal level=-65 dBm  Noise level=-85 dBm
Rx invalid nwid:19515  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

```
Envy-Laptop:/# ping -c3 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=15.1 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=1.71 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=3.94 ms

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 1.710/6.934/15.151/5.881 ms
```

Sembla que ara sí que ens deixa fer PING.

Anem a veure que ha passat amb IWEVENT.

Consola 2:

```
...
18:32:53.132435 ath0 Set Encryption key:****-****-****-****-****-****-****
18:32:53.133896 ath0 New Access Point/Cell address:Not-Associated
18:32:53.134051 ath0 Set ESSID:"Envy-TFC"
18:32:53.137290 ath0 New Access Point/Cell address:00:18:39:28:3A:70
...
```

Veiem que automàticament al introduir una nova clau WEP, el client es desassocia del Punt d'Accés i es torna a associar.

El que hem pogut comprovar és la diferència entre el procés d'associació i el de comunicació. El primer pas per la creació d'una xarxa és que el Punt d' Accés accepti que el client en formi part. És el procés d'associació i hem pogut veure la diferència entre *Open System* i *Shared Key*. El segon pas és disposar de la clau per encriptar i desencriptar les dades. Si no es disposa podem estar associats (si és *Open System*) però no podem transmetre ni rebre res.

4.4. Encriptació Avançada: WPA/WPA2

Degut a diverses vulnerabilitats i la feblesa dels mecanismes implementats inicialment per 802.11, a l'any 2004 apareixen una sèrie de mesures definides com a *Wi-Fi Protected Access* (WPA). Aquestes mesures adoptades ràpidament es convertirien més tard en la definició d'un nou estàndard específic per a seguretat, 802.11i. En ell es recullen un conjunt de tècniques que tracten principalment l'autenticació, l'encriptació i la generació de claus.

En aquest apartat revisarem a nivell teòric aquests tres aspectes però a la part pràctica ens centrarem en WPA i WPA2.

4.4.1. Conceptes teòrics

Wi-Fi Protected Access (WPA/WPA2): és un tipus de seguretat definida per xarxes *WiFi*. Va ser creat en resposta a serioses vulnerabilitats presentades pels mecanismes adoptats anteriorment amb WEP. WPA implementa la major part de l'estàndard IEEE 802.11i, i va ser dissenyat per suplir de forma ràpida les carències de WEP mentre es definia 802.11i.

WPA és dissenyat per treballar amb interfícies de xarxes *WiFi*, però no necessàriament amb la primera generació de Punts d'Accés. WPA2 implementa l'estàndard complet, però no treballa amb algunes targetes de xarxa antigues.

El mode *Pre-shared key* (PSK, també conegut com a “Mode Personal”) és dissenyat per xarxes domèstiques i d'oficina que no poden assumir els costos i la complexitat d'una xarxa amb servidor d'autenticació. Cada usuari ha d'introduir un mot de pas entre 8 i 63 caràcters ASCII o bé 64 dígits hexadecimal (256 bits).

Nota: Si utilitzem caràcters ASCII, la funció Hash els redueix a 504 bits (63 caràcters * 8 bits/caràcter) a 256 bits (utilitzant també el SSID).

El mot de pas ha de ser emmagatzemat en el PC de forma discreta, fet que hauria de garantir el sistema operatiu. Evidentment també ha d'estar emmagatzemat en el Punt d'Accés.

Autenticació: El *Four-Way Handshake* (Acord de 4 camins)

Un procés d'autenticació en xarxes *WiFi* comporta dues consideracions: per un cantó trobem el Punt d' Accés (AP) el qual encara necessita autenticar-se ell mateix respecte al client (STA), i encara necessita les claus per poder encriptar el tràfic resultant.. Les primeres versions de EAP provenien un mecanisme amb un parell de claus PMK (*Pairwise Master Key*). Aquestes claus han de ser mostrades el menys possibles.

En canvi el *4-way Handshake* és utilitzat per establir encara una segona clau, la PTK (*Pairwise Transient Key*). PTK concatenant una sèrie d'atributs: PMK, *AP nonce* (*ANonce*), *STA nonce* (*SNonce*), adreça MAC del Punt d' Accés i la adreça MAC del STA. En el resultat hi afegim un procés criptogràfic basat en *Hash*.

El *handshake* també aporta la GTK (*Group Temporal Key*), utilitzada per desencryptar tràfic *multicast* i *broadcast*. El procés d'intercanvi de missatges segueix el següent esquema:

1. El Punt d'Accés envia el *nonce-value* al STA (*ANonce*). El client disposa ara dels valors per construir la PTK.
2. El STA envia els seu *nonce-value* (*SNonce*) en el Punt d' Accés conjuntament amb el MIC.
3. El Punt d'Accés envia la GTK i el número de seqüència conjuntament amb el MIC. El número de seqüència serà el que s' utilitzarà en la propera trama *multicast* o *broadcast*, pel que el STA rebut pot realitzar una cerca bàsica.
4. El STA envia confirmació en el Punt d'Accés.

Un cop rebuda la PTK, aquesta se separa en 5 claus:

PTK (*Pairwise Transient Key* – 64 bytes)

1. 16 bytes *EAPOL-Key Encryption Key* (KEK) - AP utilitza aquesta clau per enviar dades encriptades (en el camp 'Key Data') en el client (per exemple, la RSN IE o la GTK)
2. 16 bytes *EAPOL-Key Confirmation Key* (KCK)– Utilitzada per computar MIC sobre missatges de clau WPA EAPOL.
3. 16 bytes *Temporal Key* (TK) – Utilitzada per encriptar/desencriptar paquets de dades *unicast*.
4. 8 bytes de clau MIC Autenticadora Tx (transmissió) – Utilitzada per computar MIC sobre dades *unicast* transmeses per l' AP.
5. 8 bytes de clau MIC autenticadora Rx (recepció) – Utilitzada per computar MIC sobre dades *unicast* transmeses pel client.

Les Claus MIC autenticadores Tx/Rx obtingudes en el *handshake* són només utilitzades a la xarxa si encriptem les dades amb TKIP.

La Group Key Handshake (Acord de Clau de Grup)

La GTK utilitzada en la xarxa és de duració limitada i expira passat un temps determinat. Quan un dispositiu abandona la xarxa *WiFi*, la GTK necessita ser actualitzada. Això és per a prevenir al dispositiu de no rebre més missatges del AP.

Per realitzar la actualització, 802.11i defineix el *Group Key Handshake* que consisteix en un mètode d'acord de 2 camins (*two-way handshake*):

1. El Punt d' Accés envia la nova GTK a cada STA a la xarxa. La GTK es encriptada utilitzant KEK assignada al STA i protegeix les dades de ser falsejades utilitzant MIC.
2. El STA envia ACK amb la nova GTK i respon al Punt d' Accés.

GTK (*Groupwise Transient Key* – 32 bytes)

1. 16 bytes de GTK – Utilitzada per encriptar paquets de dades *multicast*.
2. 8 bytes de clau MIC autenticadora Tx – Utilitzada per computar MIC en paquets Multicast transmesos pel AP
3. 8 bytes de clau MIC autenticadora Rx – Actualment no s'implementa a les estacions i no envia tràfic *multicast*.

Les Claus MIC autenticadores Tx/Rx obtingudes en el handshake són només

utilitzades a la xarxa si encriptem les dades amb TKIP.

Programari a utilitzar:

WPA_Supplicant: és una implementació de la part client del WPA *Supplicant* (només vàlida pel node client) . Implementa l'apartat de negociació de clau amb el WPA *Authenticator* i l'autenticació EAP amb servidor d'autenticació. També permet controlar l'autenticació amb *Roaming*, és a dir, quan el client d'una mateixa xarxa canvia de Punt d'Accés.

De les opcions disponibles de la comanda *wpa_supplicant*, en destacarem :

- B: executa l'aplicació en segon pla.
- i: indica la interfície a configurar
- D: indica el driver amb el que volem treballar

Aquests poden ser:

- *hostap* (*Intersil Prism2/2.5/3*).
- *hermes* (*Hermes-I/Hermes-II*).
- *Madwifi* (*Atheros, etc.*).
- *atmel* (*ATMEL AT76C5XXx, [USB i PCMCIA]*).
- *wext* (*Linux wireless extensions*).
- *ndiswrapper*
- *broadcom*
- *ipw* (*Intel ipw2100/2200*).
- *wired* (*wired Ethernet driver*)
- *bsd* (*Atheros, etc.*).
- *ndis* (*Windows NDIS driver*).

- c: indica el fitxer amb la configuració

Aquests són els valors disponibles del fitxer de configuració:

wpa-ssid (*SSID en text pla*): indica el SSID

wpa-bssid (*00:1a:2b:3c:4d:5e*): indica el BSSID del Punt d'Accés

wpa-psk (*64 bits en hexadecimal*) : clau predefinida de WPA.

Nota: Per obtenir una clau en hexadecimal a partir de la Paraula clau i el SSID utilitzem `wpa_passphrase [SSID] [Paraula_clau]`.

`wpa-key-mgmt` (*NONE, WPA-PSK, WPA-EAP, IEEE8021X*): llistat de claus d'autenticació.

`wpa-group` (*CCMP, TKIP WEP40, WEP104*): grups acceptats per WPA.

`wpa-pairwise` (*CCMP, TKIP, NONE*): parells de claus acceptades per WPA

`wpa-auth-alg` (*OPEN, SHARED, LEAP*): tipus d'autenticació.

`wpa-proto` (*WPA, RSN*): protocols acceptats en aquest cas indica WPA i WPA2.

`wpa-identity` (*nom en text pla, EAP authentication*): claus d'usuari previstes per l'administrador.

`wpa-password` (*password en text pla*): clau personal per autenticació EAP.

`wpa-scan-ssid` (*0 o 1*): conmuta scan de SSID amb intents de Probe Request (pot servir per detectar SSID ocults).

`wpa-ap-scan` (*0 o 1 o 2*): ens permet ajustar la lògica de *scan*.

WPA_CLI: utilitat que ens permet interaccionar amb WPA_SUPPLICANT. Un cop executat WPA_SUPPLICANT podem comprovar i modificar diferents paràmetres amb dos modes diferents: executant les comandes amb una línia o bé interactuant amb una consola.

Les opcions en són moltes (es recomana veure el manual per un estudi més detallat), però nosaltres en centrarem en 3:

`-status`: ens dona un resum dels paràmetres bàsic de la o les connexions que tenim fixades amb WPA_SUPPLICANT

`-list_networks`: ens mostra les opcions de configuració de les xarxes especificades a WPA_SUPPLICANT.CONF

`-reconfigure`: fa rellegir el fitxer de configuració de WPA_SUPPLICANT.

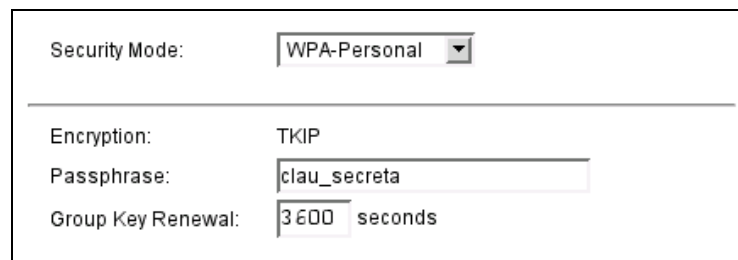
4.4.2. Objectiu

Configurar el Punt d' Accés i el client amb WPA i WPA2.

4.4.3. Realització

1. Configurem el Punt d' Accés amb WPA/Tkip

Triem aquesta opció i introduïm la paraula clau. Aquesta és compartida pel client (*Pairwise Master Key*). Amb aquesta clau el Punt d' Accés internament podrà generar la clau de transició (*Pairwise Transient Key*) per finalment obtenir la Clau temporal de grup (*Groupwise Temporal Key*). En aquest cas obtenim encriptació TKIP. Hem d'introduir una clau d'un longitud mínima de 8 caràcters i un màxim de 63. Finalment indiquem cada quan temps el Punt d' Accés ha de renovar la clau de grup (en aquest cas triem cada hora).



Security Mode:	WPA-Personal
Encryption:	TKIP
Passphrase:	clau_secret
Group Key Renewal:	3600 seconds

Imatge 15. Opcions de seguretat del Punt d'Accés (WPA)

2. Configurem el client amb WPA_Supplicant

Primer hem de preparar l'arxiu de configuració. Editem amb un editor de text l'arxiu WPA_SUPPLICANT.CONF afegint les següents línies:

```
2. network={  
    ssid="Envy-TFC"  
    bssid=00:18:39:28:3A:70  
    psk="clau_secret"  
    group=TKIP  
    pairwise=TKIP  
}
```

Hem afegit amb el camp BSSID l'adreça MAC del Punt d' Accés al que volem connectar, molt útil quan hi ha més d' un Punt d' Accés a la xarxa Envy-Net i volem forçar la connexió només a un.

Si volem posar la clau_secretà en hexadecimal podem utilitzar
WPA_PASSPHRASE:

```
Envy-Laptop # wpa_passphrase Envy-TFC clau_secretà

network={
    ssid="Envy-TFC"
    #psk="clau_secretà"
    psk=aff205c7854389d42bb335424c68be8ff416ec94f39bc67df7020b59c1a01431
}
```

Ara amb WPA_CLI comprovarem l'estat de la connexió:

Envy-Laptop # **wpa_cli**

```
wpa_cli v0.5.7
Copyright (c) 2004-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors

This program is free software. You can distribute it and/or modify it
under the terms of the GNU General Public License version 2.

Alternatively, this software may be distributed under the terms of the
BSD license. See README and COPYING for more details.

Selected interface 'ath0'

Interactive mode

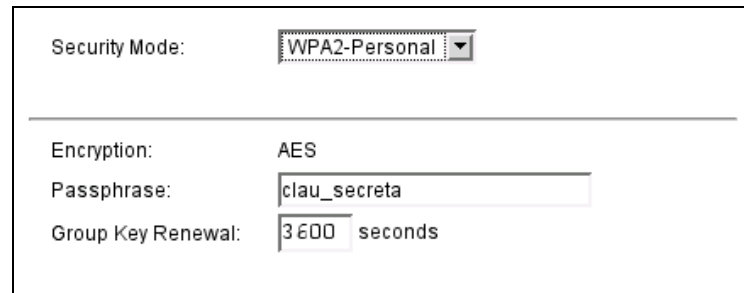
> status
bssid=00:18:39:28:3a:70
ssid=Envy-TFC
id=2
pairwise_cipher=TKIP
group_cipher=TKIP
key_mgmt=WPA-PSK
wpa_state=COMPLETED
ip_address=192.168.1.23
> quit
```

Veiem que s'ha connectat al Punt d' Accés indicat, el parell de claus i el grup és encriptat amb TKIP, l'intercanvi de claus es fa per WPA-PSK i WPA_STATE=COMPLETED ens indica que tot el procés s'ha realitzat.

***Nota:** la consola de WPA_CLI és una eina molt potent que ens permet interaccionar de forma còmode i senzilla amb WPA_SUPPLICANT.*

3. Configurem el Punt d' Accés amb WPA/AES (WPA2).

En aquest cas la única diferència amb l'apartat anterior és l'encryptació AES.

A screenshot of a network configuration interface for WPA2 security. It features a 'Security Mode' dropdown menu set to 'WPA2-Personal'. Below this, there is a section for 'Encryption' set to 'AES', a 'Passphrase' text field containing 'clau_secreta', and a 'Group Key Renewal' field set to '3600 seconds'.

Imatge 16. Opcions de seguretat del Punt d'Accés (WPA2).

Configurem el client amb *WPA_Supplicant*.

Editem amb un editor de text l'arxiu WPA_SUPPLICANT.CONF canviant només els paràmetres de GROUP i PAIRWISE (TKIP -- CCMP):

```
network={  
    ssid="Envy-TFC"  
    bssid=00:18:39:28:3A:70  
    psk="clau_secreta"  
    group=CCMP  
    pairwise=CCMP  
}
```

Comprovem l'estat amb WPA_CLI:

```
Envy-Laptop fede # wpa_cli
wpa_cli v0.5.7
Copyright (c) 2004-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors

This program is free software. You can distribute it and/or modify it
under the terms of the GNU General Public License version 2.

Alternatively, this software may be distributed under the terms of the
BSD license. See README and COPYING for more details.

Selected interface 'ath0'

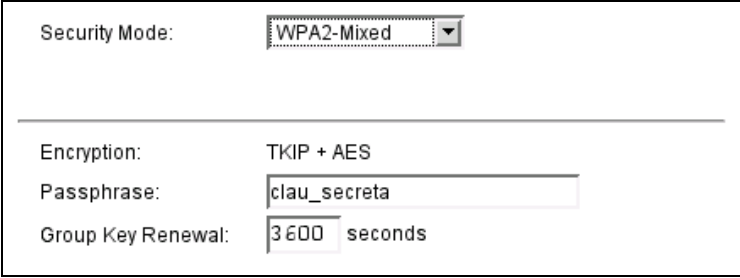
Interactive mode

> status
bssid=00:18:39:28:3a:70
ssid=Envy-TFC
id=2
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA2-PSK
wpa_state=COMPLETED
ip_address=192.168.1.2
> quit
```

Veiem que ara les opcions s'han actualitzat a WPA2 i el cifratge es fa amb CCMP combinat amb TKIP, l'algorisme d' encriptació utilitzat per AES (*Advanced Encryption System*).

5. Configurem el Punt d' Accés en mode Mixt (WPA/WPA2).

En aquest cas el Punt d' Accés permet qualsevol de les dues solucions anteriors.



The image shows a configuration window for network security. At the top, 'Security Mode' is set to 'WPA2-Mixed' in a dropdown menu. Below this, there is a horizontal separator line. Under the line, 'Encryption' is set to 'TKIP + AES'. 'Passphrase' is entered as 'clau_secreta' in a text field. 'Group Key Renewal' is set to '3600 seconds', with '3600' in a text field and 'seconds' as a label.

Security Mode:	WPA2-Mixed
Encryption:	TKIP + AES
Passphrase:	clau_secreta
Group Key Renewal:	3600 seconds

Imatge 17. Opcions de seguretat del Punt d'Accés (Mode Mixt)

En aquest apartat qualsevol de les connexions establertes anteriorment el Punt d' Accés les detecta i permet treballar amb ambdós. Per tant qualsevol configuració anterior és vàlida.

Capítol V: Anàlisi dels paquets

5.1. Descripció dels paquets

L'especificació 802.11 defineix diferents tipus de paquet que els equips utilitzen en el procés de comunicació. Bàsicament aquest els podem establir en dos classes en funció del seu ús principal:

- Management Paquets:** serveixen per intercanviar informació pròpia de la xarxa (SSID, seguretat), peticions (associació, autenticació) o informació del medi (nivell de soroll, potència).
- Control Paquets:** serveixen per canviar informació de control de *link* (si s'han rebut paquets, si el medi és net...).
- Data Paquets:** s'utilitzen per enviar la informació i en ells es poden incloure altres protocols d'altres capes.

En el següents apartats definirem més detalladament els tipus de paquets dins de cada grup, veurem els camps més rellevants i analitzarem un *Beacon Frame*.

5.1.1. Tipus de paquets

- Management Paquets (el més rellevants).

Autenticació: serveixen per realitzar el procés d'autenticació dels equips. En aquest procés el Punt d' Accés valida al client i a la inversa. Disposem de dos tipus d'autenticació: *Open System* i *Shared Key*. En el primer només enviar la petició d'autenticació el Punt d'Accés valida el client enviant la següent resposta:

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

Amb *Shared Key* quan el client sol·licita ser autenticat el Punt d'Accés envia un text de desafiament:

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
    Authentication Algorithm: Shared key (1)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
  Tagged parameters (130 bytes)
    Challenge text
      Tag Number: 16 (Challenge text)
      Tag length: 128
      Tag interpretation: Challenge text:
39846440B11AF62A1FFDF8B4822C26D9A91FBE750EBF0C48
...
```

Si el client el respon correctament (encriptant amb la clau corresponent el desafiament), el Punt d'Accés el validarà acceptant la seva petició:

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
    Authentication Algorithm: Shared key (1)
    Authentication SEQ: 0x0003
    Status code: Successful (0x0000)
```

També potser que no ens validi per posar una clau incorrecta o directament per confondre un sistema *Open System* per *Shared Key*:

```
IEEE 802.11 wireless LAN management frame

  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0002
    Status code: Responding station does not support the specified authentication algorithm (0x000d)
```

Desautenticació: és el paquet que l'estació envia a un client per desautenticar-lo de forma segura.

Petició d' Associació: habilita la radio del client per establir un procés d'associació. La petició ha d'anar acompanyada d'una resposta indicant les paràmetres que el Punt d'Accés té prefixats. Per exemple, el *bitrate*,

```
IEEE 802.11

Type/Subtype: Association Request (0)
Frame Control: 0x0000 (Normal)
  Version: 0
  Type: Management frame (0)
  Subtype: 0
  Flags: 0x0
Duration: 314
Destination address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Source address: 00:02:6f:20:18:e5 (00:02:6f:20:18:e5)
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Fragment number: 0
Sequence number: 226
IEEE 802.11 wireless LAN management frame
  Fixed parameters (4 bytes)
  Tagged parameters (30 bytes)
    SSID parameter set: "Envy-TFC"
    Supported Rates: 1.0 (B) 2.0 (B) 5.5 (B) 6.0 9.0 11.0 (B) 12.0 18.0
    Power Capability: Tag 33 Len 2
    Extended Supported Rates: 24.0 36.0 48.0 54.0
```

frequència i potència.

Resposta d' Associació: el client respondrà amb amb els seus paràmetres i ajustarà la resta automàticament.

```
IEEE 802.11

Type/Subtype: Association Response (1)
Frame Control: 0x0010 (Normal)
  Version: 0
  Type: Management frame (0)
  Subtype: 1
  Flags: 0x0
Duration: 212
Destination address: 00:02:6f:20:18:e5 (00:02:6f:20:18:e5)
Source address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Fragment number: 0
Sequence number: 2249
IEEE 802.11 wireless LAN management frame
Fixed parameters (6 bytes)
Tagged parameters (16 bytes)
  Supported Rates: 1.0 (B) 2.0 (B) 5.5 (B) 6.0 9.0 11.0 (B) 12.0 18.0
  Extended Supported Rates: 24.0 36.0 48.0 54.0
```

Petició de Proba: s'envia d'un equip a *broadcast* quan es necessita obtenir

```
IEEE 802.11

Type/Subtype: Probe Request (4)
Frame Control: 0x0040 (Normal)
Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
  Source address: 00:11:50:3e:80:d9 (00:11:50:3e:80:d9)
  BSS Id: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Fragment number: 0
Sequence number: 930
IEEE 802.11 wireless LAN management frame
```

informació del equips veïns.

Resposta de Proba: en la resposta s'envia la informació demanada seguint sempre la mateixa estructura.

```
IEEE 802.11

Type/Subtype: Probe Response (5)
Frame Control: 0x0850 (Normal)
  Version: 0
  Type: Management frame (0)
  Subtype: 5
  Flags: 0x8
Duration: 316
Destination address: 00:11:50:3e:80:d9 (00:11:50:3e:80:d9)
Source address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Fragment number: 0
Sequence number: 1059
```

En Control paquets.

Request to Send: ajuda a reduir les colisions de paquets tot i ser un paràmetre opcional. Demana a priori si és possible l'enviament abans de l'enviament de dades la qual és retornada amb un **Clear to Send:**

```
IEEE 802.11

Type/Subtype: Clear-to-send (28)
Frame Control: 0x00C4 (Normal)
Duration: 90
Receiver address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
```

Ack: si no hi ha errors en els paquets rebuts, l'estació receptora envia un ACK indicant que la comunicació s'ha rebut correctament:

```
IEEE 802.11

Type/Subtype: Acknowledgement (29)
Frame Control: 0x00D4 (Normal)
Duration: 0
Receiver address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
```

En paquets de dades.

Serveixen per transportar la informació. En funció de si s'utilitza encriptació podem veure la informació que inclou.

Veiem com és un paquet quan fem *ping* en una xarxa sense encriptació:

```
IEEE 802.11

Type/Subtype: Data (32)
Frame Control: 0x0108 (Normal)
Version: 0
Type: Data frame (2)
Subtype: 0
Flags: 0x1
Duration: 44
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Source address: 00:02:6f:20:18:e5 (00:02:6f:20:18:e5)
Destination address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Fragment number: 0
Sequence number: 1717
Logical-Link Control
Internet Protocol, Src: 192.168.1.23 (192.168.1.23), Dst: 192.168.1.1
(192.168.1.1)
Internet Control Message Protocol
```

Veiem com el paquet encapsula la petició de PING.

```
IEEE 802.11
Type/Subtype: Data (32)
Frame Control: 0x4208 (Normal)
  Version: 0
  Type: Data frame (2)
  Subtype: 0
  Flags: 0x42
Duration: 44
Destination address: 00:02:6f:20:18:e5 (00:02:6f:20:18:e5)
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Source address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Fragment number: 0
Sequence number: 2287
WEP parameters
  Initialization Vector: 0xad927e
  Key Index: 0
  WEP ICV: 0x8d7d81cf (not verified)
Data (584 bytes)

0000  1a 06 be 28 8d a8 1b a3 34 b5 4c 78 5b e1 f2 90  ...(.4.Lx[...
0010  56 09 6d 31 fb 37 18 de d7 5a 4a 56 a5 07 f4 04  V.m1.7...ZJV....
0020  66 f3 5e e0 86 19 50 3e fa 13 ce 60 da 50 3a 63  f.^...P>...`.P:c
0030  6f 0a d3 83 9d 90 69 c2 c4 8e 3c 39 1a 33 18 ce  o.....i...<9.3..
0040  14 ed b0 a8 b8 b3 a6 e4 0f 03 6e 55 bb 51 f5 c1  .....nU.Q..
0050  c2 11 28 db 25 2e 85 b2 88 e3 98 d7 e4 4d 37 97  ..(.%.....M7.
0060  55 1c 54 47 3d c4 b8 c6 b5 85 65 97 f6 aa ab b5  U.TG=.....e.....
0070  f3 cc ab f7 ba 40 eb 42 40 00 25 e3 41 eb 2d 78  .....@.B@.%.A.-x
0080  7b f5 1d 7e fd 53 92 b7 3b 07 9a 1e 1f 52 76 14  {...~.S.;....Rv.
0090  0d 97 5c 61 4c 41 00 c1 6d 37 b7 ac c3 a6 8f 80  ..\aLA..m7.....
[...]
```

Veiem com ara les dades estan encriptades. El paquet envia el vector d'inicialització, l'índex de clau i el ICV. Tot seguit envia les dades encriptades (el mateix *ping* d'abans).

5.1.2. Anàlisi d'un Beacon Frame

L'objectiu del següent apartat és aprendre a snifar tràfic *WiFi*. Per fer-ho aprendrem a treballar en mode Monitor amb les *Wireless Tools* i amb el *Driver* de *MadWiFi*. Crearem un VAP (*Virtual Acces Point*) per facilitar el procés de snifat. Finalment capturarem i analitzarem un *Beacon Frame* com a mostra més detallada d'un paquet *WiFi*.

Realització

1. **Configurem el Punt d'Accés (veure Capítol 3).**
2. **Configurem la interfície *WiFi* en mode *Monitor*.**
 - *Opció 1*: utilitzem les *Wireless Tools*.

```
Envy-Laptop # iwconfig eth1 mode monitor
```

- *Opció 2*: utilitzem el *Driver MadWiFi* (només per targetes *Atheros*).

Creem un VAP (*Virtual Access Point*), una nova interfície en la mateixa targeta. Això ens permet tenir més d'una interfície en un mateix dispositiu.

```
Envy-Laptop # wlanconfig ath create wlandev wifi0 wlanmode monitor
```

Amb IWCONFIG podem veure la nova interfície.

```
Envy-Laptop # iwconfig

eth0      no wireless extensions.

lo        no wireless extensions.

wifi0     no wireless extensions.

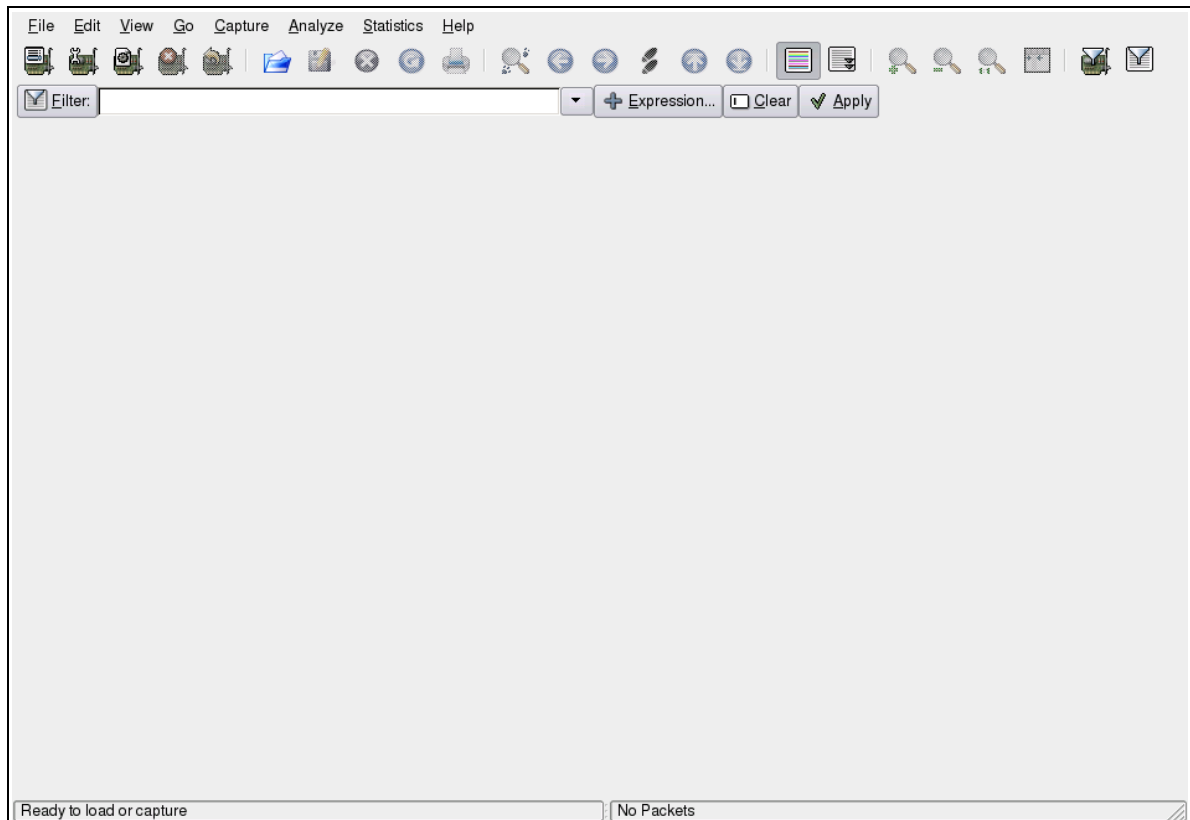
ath0      IEEE 802.11a  ESSID:"Envy-TFC"
          Mode:Managed  Frequency:5.3 GHz  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:15 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-96 dBm  Noise level=-96 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

ath8      IEEE 802.11a  ESSID:""
          Mode:Monitor  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:15 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-96 dBm  Noise level=-96 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Podem comprovar com la interfície ATH8 s'ha creat en mode *monitor*. Això ens permetrà snifar tràfic al mateix temps que podem realitzar connexions al Punt d'Accés.

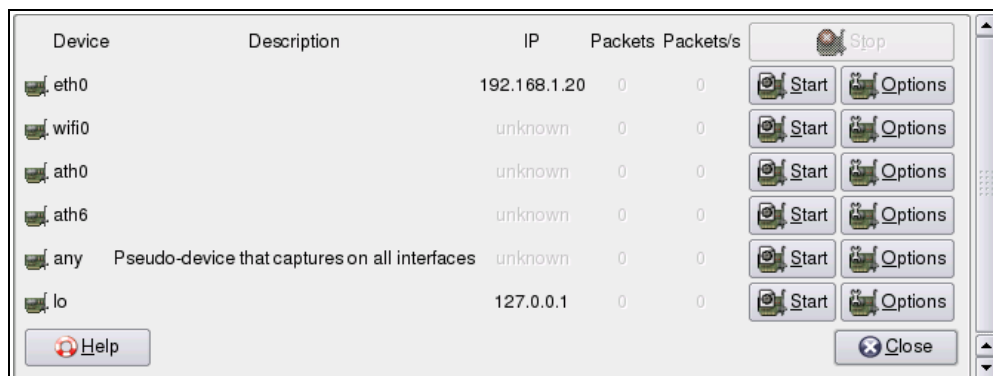
3. Utilitzar un Analitzador de Xarxes.

En aquest cas utilitzem *Wireshark* (antic *Ethereal*) ja que ens permet una còmode visualització a més de l'ús de filtres.



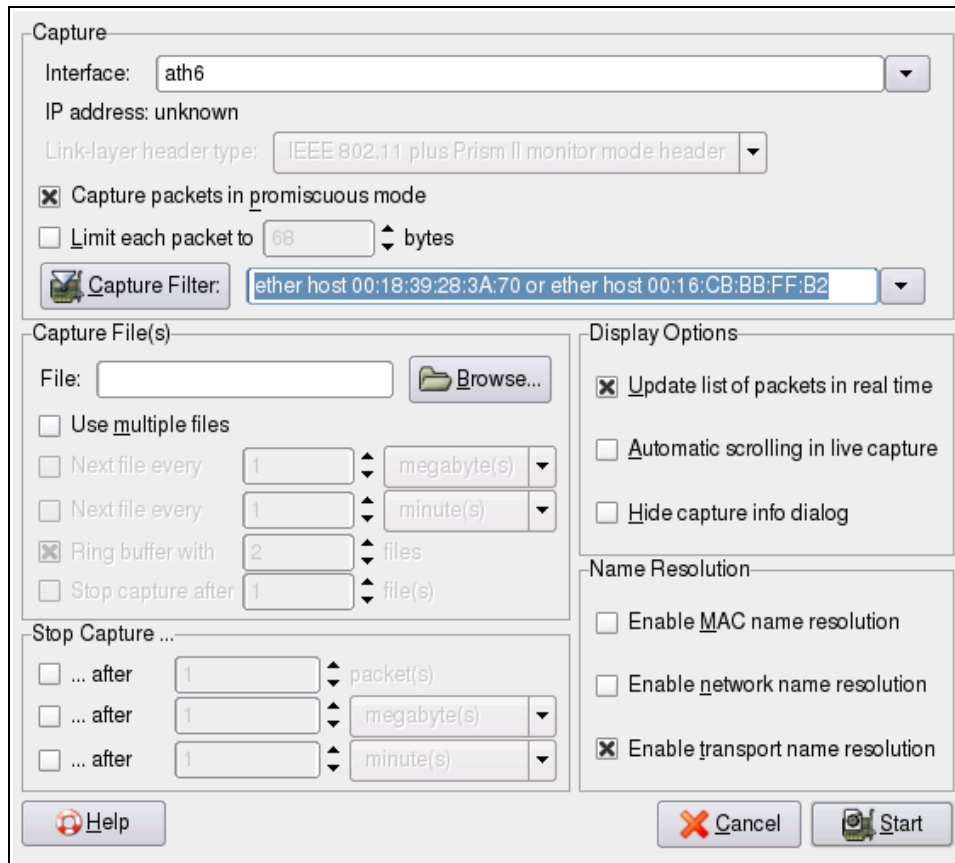
Imatge 18. Analitzador WireShark

Dins el Menú seleccionem *Capture – Interfaces* .



Imatge 19. Analitzador WireShark (Interfícies)

Busquem la interfície que tenim en mode *Monitor* i seleccionem *Options*.



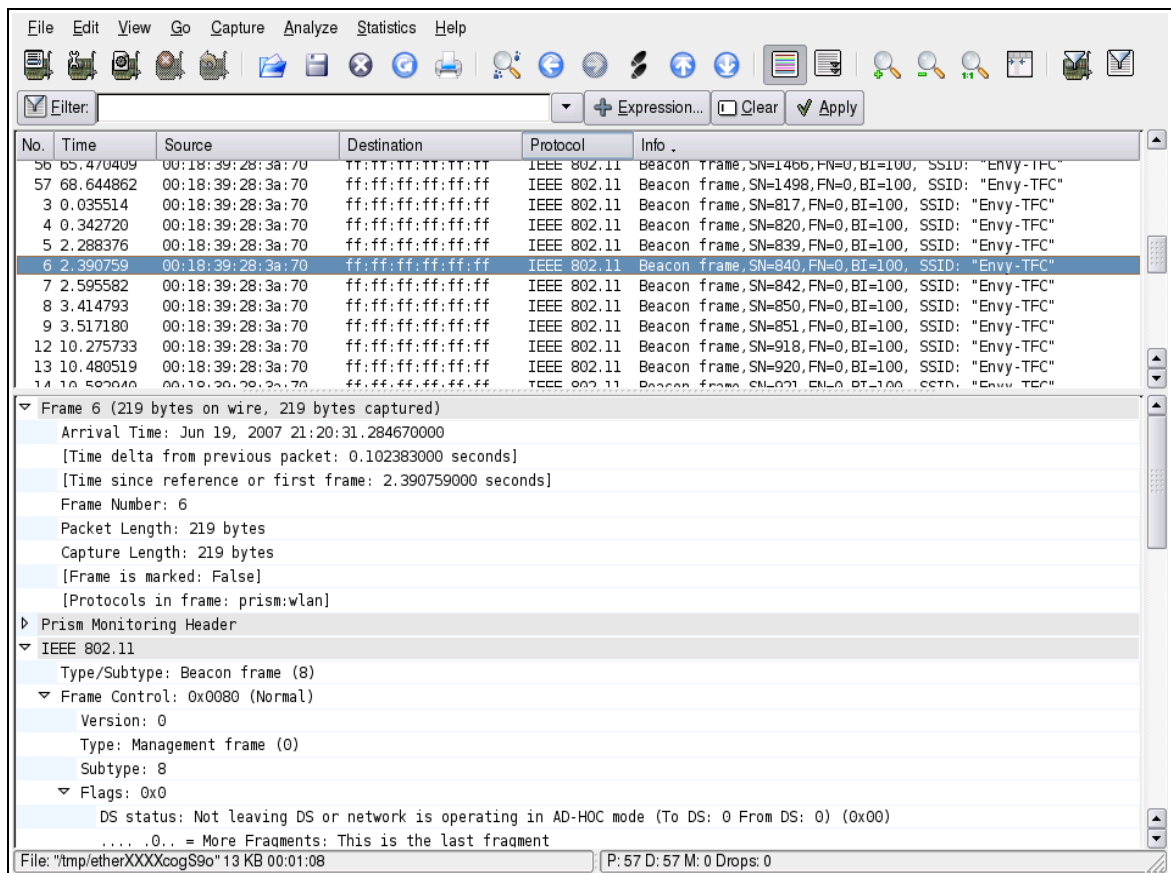
Imatge 20. Analitzador WireShark (Filtres)

En aquest apartat podem establir filtres de manera que només snifem els paquets que ens interessin. Si ens trobem en un medi on hi ha molt de tràfic podríem trobar-nos amb molts paquets que ens dificultarien l'anàlisi. Posant filtres podem centrar-nos amb el tràfic que ens interessa. Filtrarem per adreça MAC, ens centrarem amb els paquets enviats o rebuts pel Punt d' Accés i/o el Client amb la següent expressió:

```
ether host "MAC Punt d' Accés" or ether host "MAC client"
```

Tot seguit cliquem *Start* i podrem veure com en tant sols uns segons obtindrem unes desenes de paquets. Si només tenim configurat el Punt d'Accés, obtindrem *Beacon Frames* anunciant els diferents AP que puguin estar connectats.

NOTA: els Beacon Frames s'envien en Broadcast, per tant el filtre els accepta.



Imatge 21. Analitzador WireShark (Paquets)

Podrem veure a la part superior, a mode de resum, els paquets snifats.

- *Adreça Origen (Source)*: adreça MAC de l'equip que envia el paquet.
- *Adreça Destí (Destination)*: adreça MAC de l'equip destinat. FF:FF:FF:FF:FF:FF indica que és un paquet de *Broadcast* i que el rep tothom.
- *Protocol*: indica a quin protocol pertany, en el nostre cas 802.11.
- *Descripció (info)*: ens indica a mode resum detalls rellevants del paquet.

Cercarem paquets *BEACON FRAMES* on el SSID sigui Envoy-TFC. Triat un paquet podem veure en la part inferior de la pantalla explicació detallada de tots els camps del paquet i la informació que transporta. Anem a veure la informació més rellevant d' un *Beacon Frame*.

Prism Monitoring Header

```
Message Code: 68
Message Length: 144
Device: ath8
Host Time: 0xa473c (DID 0x10044, Status 0x0, Length 0x4)
MAC Time: 0xa29c1c46 (DID 0x20044, Status 0x0, Length 0x4)
Channel: 0x2 (DID 0x30044, Status 0x0, Length 0x4)
RSSI: 0xa (DID 0x40044, Status 0x0, Length 0x4)
SQ: 0x0 (DID 0x0, Status 0x0, Length 0x0)
Signal: 0xffffffffb4 (DID 0x60044, Status 0x0, Length 0x4)
Noise: 0xfffffffffaa (DID 0x70044, Status 0x0, Length 0x4)
Data Rate: 2.0 Mb/s
IsTX: 0x0 (DID 0x90044, Status 0x0, Length 0x4)
Frame Length: 0x4f (DID 0xa0044, Status 0x0, Length 0x4)
```

Aquesta és la capçalera de monitorització. L'afegeix la interfície nostra i ens dóna informació del canal, la senyal, el nivell de soroll. Els valors són en hexadecimal i serveix al *driver* i al *chipset* de la targeta per poder després mostrar els valors de IWCONFIG.

IEEE 802.11

```

Type/Subtype: Beacon frame (8)
Frame Control: 0x0080 (Normal)
Version: 0
Type: Management frame (0)
Subtype: 8
Flags: 0x0
    DS status: Not leaving DS or network is operating
               in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = Order flag: Not strictly ordered
Duration: 0
Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Source address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Fragment number: 0
Sequence number: 2521

```

Aquesta és la capçalera pròpia de 802.11.

- *Version, type i subtype*: ens indica quin tipus de paquet es tracta. Pertany a MANAGEMENT FRAME concretament del tipus 8, és a dir, un BEACON FRAME.
- *Flags*: mitjançant estats (actiu/no actiu) ens informa de si és l'últim fragment, si és un paquet retransmès, si hi ha algun client actiu en la xarxa, si hi ha informació en buffer, si està encriptat i si està ordenat. Com que el Punt d' Accés no té cap client connectat, DS està a 0.
- *Destination address*: ens diu a qui va destinat el paquet. En aquest cas a tothom ja que és *broadcast*.
- *Source address i BSS id*: són l'adreça MAC del Punt d' Accés.

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x0000000EDFD4B155

Beacon Interval: 0.102400 [Seconds]

Capability Information: 0x0421

.... 1 = ESS capabilities: Transmitter is an AP

.... 0 = IBSS status: Transmitter belongs to a BSS

.... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)

.... 0 = Privacy: AP/STA cannot support WEP

.... 1 = Short Preamble: Short preamble allowed

.... 0.. = PBCC: PBCC modulation not allowed

.... 0... = Channel Agility: Channel agility not in use

.... 0 = Spectrum Management: dot11SpectrumManagementRequired FALSE

.... 1.. = Short Slot Time: Short slot time in use

.... 0... = Automatic Power Save Delivery: apsd not implemented

..0. = DSSS-OFDM: DSSS-OFDM modulation not allowed

.0.. = Delayed Block Ack: delayed block ack not implemented

0... = Immediate Block Ack: immediate block ack not implemented

En aquí s'informa de paràmetres que suporta el Punt d' Accés. En ells es parla de modulacions suportades, control d' potència a més d'altres factors. Cal destacar el camp de *Privacy* el qual ens indica que no hi ha WEP activat.

Tagged parameters (39 bytes)

SSID parameter set: "Envy-TFC"

Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 22.0

DS Parameter set: Current Channel: 11

(TIM) Traffic Indication Map: DTIM 0 of 1 bitmap empty

ERP Information: no Non-ERP STAs, do not use protection, short or long preambles

Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

En aquest apartat és on trobem la informació rellevant del Punt d'Accés. En aquí se'ns informa del SSID de la xarxa, les velocitats que se suporten, el canal pel qual es transmet i que no s'utilitza cap mesura de protecció.

5.2. Vulnerabilitats

Amb aquest darrer apartat i amb els coneixements apresos anteriorment, veurem com les mesures de seguretat aplicades per 802.11b presenten greus vulnerabilitats. Ho mostrarem amb 3 exemples pràctics que ens ajudaran a veure per nosaltres mateixos la debilitat i incoherència d'aquestes mesures.

5.2.1. Esbrinar SSID Ocults (CNCP)

- Posem el Client-1 amb la interfície en mode *Monitor* a snifar.
- Configurem una xarxa amb CNAC i connectem el Client-2 al Punt d'Accés
- Un cop associats, parem de snifar i analitzem la captura amb l'Analitzador (*Wireshark*)
- Identifiquem qualsevol Management Frame, la secció *IEEE 802.11 wireless LAN management frame – Tagged Parameters*.

```
Tagged parameters (33 bytes)
```

```
SSID parameter set: "Envy-TFC"
```

```
Supported Rates: 1.0 (B) 2.0 (B) 5.5 (B) 11.0 (B) 22.0
```

```
DS Parameter set: Current Channel: 11
```

```
ERP Information: no Non-ERP STAs, do not use protection, long preambles
```

```
Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

Podem identificar clarament el SSID.

***Nota:** hi ha programes els quals detecten automàticament SSID ocults, com per exemple Kismet.*

5.2.2. Esbrinar MAC permeses (ACL)

- Posem el Client-1 en mode *Monitor* a snifar.
- Configurem una xarxa amb ACL, afegim la MAC del Client-2 a la llista i el connectem al Punt d' Accés.
- Un cop associats, fem *ping* del Client-2 al Punt d'Accés, parem de snifar i analitzem la captura amb l'Analitzador (*Wireshark*).
- Identifiquem qualsevol paquet de dades els camps *Source Address / Destination Address*.

```
IEEE 802.11

Type/Subtype: Data (32)
Frame Control: 0x0108 (Normal)
  Version: 0
  Type: Data frame (2)
  Subtype: 0
  Flags: 0x1
Duration: 44
BSS Id: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
Source address: 00:02:6f:20:18:e5 (00:02:6f:20:18:e5)
Destination address: 00:18:39:28:3a:70 (00:18:39:28:3a:70)
```

Sabem que el client és el *Source Address* perquè el *Destination Address* coincideix amb el BSS id el qual ens dona la MAC del Punt d'Accés.

5.2.3. Esbrinar la clau de cifratge (WEP)

Necessitem 1 Punt d'Accés i 3 Clients:

- Client-1: snifarà el tràfic i desxifrarà la clau WEP
- Client-2, Client-3: generaran tràfic.

- **Configurem el Client-1 en mode Monitor i el posem a snifar amb AERODUMP-NG.**

Hem indicat a Aerodump-ng que snifi en el canal 11, ho escrigui tot en un arxiu que el seu nom començarà per CAPTURA_WEP_ i a més li hem indicat la interfície per snifar ATH10.

```
Envy-Laptop # airodump-ng --channel 11 --write CAPTURA_WEP_ ath10
```

- **Configurem el Punt d'Accés amb un *Fragmentation Threshold* a 1000 (tamany màxim del paquet de dades).**

D'aquesta manera per transmetre la mateixa informació generarem més paquets el que ens agilitzarà el procés. A més posem una clau WEP de 64 bits: **11-22-33-44-55**.

- **Realitzem una connexió entre el Client-2 i el Client-3 que generi dades.**

En el nostre cas utilitzem una connexió SFTP, realitzant una transferència de 80MB en total.

- **Observem la consola del Client-1 on tenim AERODUMP-NG treballant.**

CH 11][Elapsed: 8 mins][2007-06-20 19:22										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	
ESSID										
00:18:39:28:3A:70	71	100	4832	297768 1581	11	54.	WEP	WEP	PSK	
Envy-TFC										
00:11:50:F9:58:B0	9	92	3911	0 0	11	11.	WPA2	CCMP	PSK	
PRIVADO										
00:03:C9:D1:FD:11	2	1	782		30	0	11	48	OPN	
Comtrend										
00:03:C9:D1:FE:81	0	0	147		1	0	11	48	OPN	
Comtrend										
BSSID	STATION		PWR	Lost	Packets	Probes				
00:18:39:28:3A:70	00:02:6F:20:18:E5		29	532	336082					
00:03:C9:D1:FD:11	00:12:F0:3C:06:FE		3	0	5	Comtrend				
00:03:C9:D1:FD:11	00:18:DE:64:F6:8F		-1	0	26					

La informació que ens mostra és la dels equips que ha trobat en el Canal 11. En nostre cas ens interessa la xarxa Envy-TFC. Els comptadors van indicant el percentatge de paquets vàlids per esbrinar la clau i la seguretat d'encert. En el nostre cas, després d'uns minuts i amb quasi 300 mil paquets, disposa d'un 71 % de paquets vàlids i una probabilitat d'encert del 100%.

- **Obrim una segona consola i cridem a AIRCRACK-NG.**

```
Envy-Laptop# aircrack-ng -a 1 -e Envy-TFC -b 00:18:39:28:3A:70 -n 64 -i 1
CAPTURA_WEP_-02.cap
```

- Ens apareix una pantalla amb els resultats del procés.

```
Aircrack-ng 0.7

[00:00:00] Tested 86 keys (got 288730 IVs)

KB    depth  byte(vote)
0    0/ 6    11( 40) CB( 25) 06( 20) 5B( 15) EE( 13) 95( 12) 59( 5) 81( 5) A6( 5) D6( 5) F2( 5) 94( 4)
1    0/ 11   22( 36) 39( 28) 91( 24) 00( 13) 3A( 13) 90( 13) F1( 13) 5A( 12) A4( 12) C8( 12) 4D( 8) 1F( 6)
2    1/ 6    37( 13) 5C( 12) A6( 12) BB( 12) 6F( 10) 29( 8) A7( 8) F9( 8) 49( 5) 68( 5) 7A( 5) 45( 4)

KEY FOUND! [ 11:22:33:44:55 ] (ASCII: ."3DU )
```

Veiem que Aircrack-ng no ha necessitat pràcticament temps per esbrinar la clau correcta. Ens dona la clau en hexadecimal que hem introduït: **11-22-33-44-55** i la corresponent Paraula Clau: **."3DU**

Cal remarcar que hem provocat les condicions ideals per agilitzar el procés d'esbrinament de clau, de manera que amb uns minuts la puguem descobrir. Aquestes condicions han estat:

- *Elevat nombre de paquets:* hem canviat el *Fragmentation Threshold* a de 2346 a 1000 provocant d'aquesta manera que per el mateix volum de dades es generin més paquets. Igualment hem realitzat una transferència SFTP la qual genera més informació que el volum de dades FTP ja que aquest primer ha d'encriptar la informació. Si es generen més paquets, podem obtenir més IV (vectors d'inicialització febles) i descobrir abans la clau.
- *Clau de 64 bits feble:* hem triat l'encriptat més feble. Tenint en

compte que la capçalera ja ens ocupa 24 bits, només queden per l'enciptació 40 bits, reduint enormement les probabilitats en un atac de força bruta. A més hem introduït una clau hexadecimal senzilla.

Malgrat tot això no vol dir que hi hagin claus WEP invulnerables: tot i tenir una bona clau en les pitjors condicions, sempre es pot esbrinar la clau en un temps raonable (en hores, màxim dies).

Capítol VI: Conclusions

Un cop finalitzat les conclusions es poden definir des de dos punts de vista:

- **A nivell d'objectius:**
 - Els document presenta el material necessari perquè d' ell en puguin sorgir unes pràctiques que es puguin posar en marxa.
 - Tot i mantenir el format de Treball Fi de Carrera, els temes exposats es presenten eminentment pràctics emprant només la base teòrica necessària per dur a terme els exercicis que es proposen.
 - Es comença assumint un nivell mínim de coneixements *WiFi*, augmentant gradualment el nivell de dificultat amb exercicis dissenyats de forma continua. Malgrat tot algú amb coneixements més avançats es pot centrar directament en pràctiques més avançades sense necessitat de realitzar les anteriors.
 - Tots els temes tractats es poden implementar amb un Punt d'Accés domèstic i dues targetes *WiFi*. Fins hi tot s'explica la possibilitat de simular més d'una interfície *WiFi* només amb un sol dispositiu (només vàlid per determinats equips).

Totes els exercicis es poden realitzar amb eines lliures que a part de ser gratuït, es pot estudiar, copiar i modificar adaptant-lo a les teves necessitats.
 - La majoria de distribucions de GNU/Linux incorporen pre-configurades les eines amb les que treballem pel qual no ens hem de preocupar per les possibles configuracions.

- **A nivell personal:**

- El projecte m'ha permès revisar i aprofundir la majoria de conceptes WiFi, revisant els estàndard i les eines per poder-los explicar.
- He pogut experimentar la dificultat de preparar unes pràctiques, jugant amb els factors que s'han de tenir en compte, els objectius que es volen assolir, els materials de que es disposen i els coneixements que es volen transmetre, sense descuidar de fer unes pràctiques interessants i divertides.

Bibliografia

- [1] <http://en.wikipedia.org/wiki/Wi-Fi> Wikipedia, *WiFi*, Abril 2007.
- [2] http://en.wikipedia.org/wiki/IEEE_802.11 Wikipedia, *802.11*, Abril 2007
- [3] http://en.wikipedia.org/wiki/Wireless_LAN Wikipedia, *WLAN*, Abril 2007
- [4] <http://en.wikipedia.org/wiki/SSID> Wikipedia, *SSID*, Abril 2007
- [5] http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing Wikipedia, *Orthogonal Frequency Division Multiplexing*, Abril 2007
- [6] http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum Wikipedia, *Direct Sequence Spread Spectrum*, Abril 2007
- [7] http://en.wikipedia.org/wiki/Complementary_code_keying Wikipedia, *Complementary Code Keying*, Abril 2007
- [8] http://en.wikipedia.org/wiki/Mobile_ad-hoc_network Wikipedia, *Mobile Ad-Hoc Network*, Abril 2007
- [9] <http://documentacion.matarowireless.net> , “(In)seguridad en redes 802.11b”, Pau Oliva Fora, Març 2003.
- [10] <http://aircrack-ng.org> , “Documentation of Aircrack Suite”, Aircrack Team, Maig 2007

Apèndix A: Manuals

IWCONFIG i IWLIST

Author: Jean Tourrilhes - jt@hpl.hp.com

Extret dels manuals de GNU/Linux

NAME

`iwconfig` - configure a wireless network interface

SYNOPSIS

iwconfig [*interface*]

iwconfig *interface* [**essid** *X*] [**nwid** *N*] [**mode** *M*] [**freq** *F*]

 [**channel** *C*][**sens** *S*][**ap** *A*][**nick** *NN*]

 [**rate** *R*] [**rts** *RT*] [**frag** *FT*] [**txpower** *T*]

 [**enc** *E*] [**key** *K*] [**power** *P*] [**retry** *R*]

 [**commit**]

iwconfig --help

iwconfig --version

DESCRIPTION

Iwconfig is similar to **ifconfig(8)**, but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation (for example : the frequency). **Iwconfig** may also be used to display those parameters, and the wireless statistics (extracted from */proc/net/wireless*).

All these parameters and statistics are device dependent. Each driver will provide only some of them depending on hardware support, and the range of values may change. Please refer to the man page of each device for details.

PARAMETERS

essid Set the ESSID (or Network Name - in some products it may also be

called Domain ID). The ESSID is used to identify cells which are part of the same virtual network.

As opposed to the AP Address or NWID which define a single cell, the ESSID defines a group of cells connected via repeaters or infrastructure, where the user may roam transparently.

With some cards, you may disable the ESSID checking (ESSID promiscuous) with *off* or *any* (and *on* to reenable it).

If the ESSID of your network is one of the special keywords (*off*, *on* or *any*), you should use *--* to escape it.

Examples :

```
iwconfig eth0 essid any  
iwconfig eth0 essid "My Network"  
iwconfig eth0 essid -- "ANY"
```

nwid/domain

Set the Network ID (in some products it may also be called Domain ID). As all adjacent wireless networks share the same medium, this parameter is used to differentiate them (create logical colocated networks) and identify nodes belonging to the same cell.

This parameter is only used for pre-802.11 hardware, the 802.11 protocol uses the ESSID and AP Address for this function.

With some cards, you may disable the Network ID checking (NWID promiscuous) with *off* (and *on* to reenable it).

Examples :

```
iwconfig eth0 nwid AB34  
iwconfig eth0 nwid off
```

freq/channel

Set the operating frequency or channel in the device. A value below 1000 indicates a channel number, a value greater than 1000 is a frequency in Hz. You may append the suffix k, M or G to the value (for example, "2.46G" for 2.46 GHz frequency), or add enough '0'.

Channels are usually numbered starting at 1, and you may use **iwlist(8)** to get the total number of channels, list the available frequencies, and display the current frequency as a channel. Depending on regulations, some frequencies/channels may not be available.

When using Managed mode, most often the Access Point dictates the channel and the driver may refuse the setting of the frequency. In Ad-Hoc mode, the frequency setting may only be used at initial cell creation, and may be ignored when joining an existing cell.

You may also use *off* or *auto* to let the card pick up the best channel (when supported).

Examples :

```
iwconfig eth0 freq 2422000000
```

```
iwconfig eth0 freq 2.422G
```

```
iwconfig eth0 channel 3
```

```
iwconfig eth0 channel auto
```

sens Set the sensitivity threshold. This is the lowest signal level for which the hardware will consider receive packets usable. Positive values are assumed to be the raw value used by the hardware or a percentage, negative values are assumed to be dBm. Depending on the hardware implementation, this parameter may control various functions.

This parameter may control the receive threshold, the lowest signal level for which the hardware attempts packet reception, signals weaker than this are ignored. This may also controls the defer threshold, the lowest signal level for which the hardware considers the channel busy. Proper setting of those threshold prevent the card to waste time receiving background noise. Modern designs seems to control those thresholds automatically.

On modern cards, this parameter may control handover/roaming threshold, the lowest signal level for which the hardware remains associated with the current Access Point. When the sig-

nal level goes below this threshold the card starts looking for a new/better Access Point.

Example :

```
iwconfig eth0 sens -80
```

mode Set the operating mode of the device, which depends on the network topology. The mode can be *Ad-Hoc* (network composed of only one cell and without Access Point), *Managed* (node connects to a network composed of many Access Points, with roaming), *Master* (the node is the synchronisation master or acts as an Access Point), *Repeater* (the node forwards packets between other wireless nodes), *Secondary* (the node acts as a backup master/repeater), *Monitor* (the node is not associated with any cell and passively monitor all packets on the frequency) or *Auto*.

Example :

```
iwconfig eth0 mode Managed
```

```
iwconfig eth0 mode Ad-Hoc
```

ap Force the card to register to the Access Point given by the address, if it is possible. When the quality of the connection goes too low, the driver may revert back to automatic mode (the card selects the best Access Point in range).

You may also use *off* to re-enable automatic mode without changing the current Access Point, or you may use *any* or *auto* to force the card to reassociate with the currently best Access Point.

Example :

```
iwconfig eth0 ap 00:60:1D:01:23:45
```

```
iwconfig eth0 ap any
```

```
iwconfig eth0 ap off
```

nick[name]

Set the nickname, or the station name. Some 802.11 products do define it, but this is not used as far as the protocols (MAC,

IP, TCP) are concerned and completely useless as far as configuration goes. Only some diagnostic tools may use it.

Example :

```
iwconfig eth0 nickname "My Linux Node"
```

rate/bit[rate]

For cards supporting multiple bit rates, set the bit-rate in b/s. The bit-rate is the speed at which bits are transmitted over the medium, the user speed of the link is lower due to medium sharing and various overhead.

You may append the suffix k, M or G to the value (decimal multiplier : 10^3 , 10^6 and 10^9 b/s), or add enough '0'. Values below 1000 are card specific, usually an index in the bit-rate list. Use *auto* to select automatic bit-rate mode (fallback to lower rate on noisy channels), which is the default for most cards, and *fixed* to revert back to fixed setting. If you specify a bit-rate value and append *auto*, the driver will use all bit-rates lower and equal than this value.

Examples :

```
iwconfig eth0 rate 11M
```

```
iwconfig eth0 rate auto
```

```
iwconfig eth0 rate 5.5M auto
```

rts[_threshold]

RTS/CTS adds a handshake before each packet transmission to make sure that the channel is clear. This adds overhead, but increases performance in case of hidden nodes or a large number of active nodes. This parameter sets the size of the smallest packet for which the node sends RTS ; a value equal to the maximum packet size disables the mechanism. You may also set this parameter to *auto*, *fixed* or *off*.

Examples :

```
iwconfig eth0 rts 250
```

iwconfig eth0 rts off

frag[mentation_threshold]

Fragmentation allows to split an IP packet in a burst of smaller fragments transmitted on the medium. In most cases this adds overhead, but in a very noisy environment this reduces the error penalty and allow packets to get through interference bursts.

This parameter sets the maximum fragment size ; a value equal to the maximum packet size disables the mechanism. You may also set this parameter to *auto*, *fixed* or *off*.

Examples :

iwconfig eth0 frag 512

iwconfig eth0 frag off

key/enc[ryption]

Used to manipulate encryption or scrambling keys and security mode.

To set the current encryption key, just enter the key in hex digits as *XXXX-XXXX-XXXX-XXXX* or *XXXXXXXX*. To set a key other than the current key, prepend or append *[index]* to the key itself (this won't change which is the active key). You can also enter the key as an ASCII string by using the *s:* prefix.

Passphrase is currently not supported.

To change which key is the currently active key, just enter *[index]* (without entering any key value).

off and *on* disable and reenale encryption.

The security mode may be *open* or *restricted*, and its meaning depends on the card used. With most cards, in *open* mode no authentication is used and the card may also accept non-encrypted sessions, whereas in *restricted* mode only encrypted sessions are accepted and the card will use authentication if available.

If you need to set multiple keys, or set a key and change the active key, you need to use multiple **key** directives. Arguments

can be put in any order, the last one will take precedence.

Examples :

```
iwconfig eth0 key 0123-4567-89
iwconfig eth0 key [3] 0123-4567-89
iwconfig eth0 key s:password [2]
iwconfig eth0 key [2]
iwconfig eth0 key open
iwconfig eth0 key off
iwconfig eth0 key restricted [3] 0123456789
iwconfig eth0 key 01-23 key 45-67 [4] key [4]
```

power Used to manipulate power management scheme parameters and mode.

To set the period between wake ups, enter *period value* . To set the timeout before going back to sleep, enter *timeout*

value . You can also add the *min* and *max* modifiers. By default, those values are in seconds, append the suffix m or u to specify values in milliseconds or microseconds. Sometimes, those values are without units (number of beacon periods, dwell or similar).

off and *on* disable and reenale power management. Finally, you may set the power management mode to *all* (receive all packets), *unicast* (receive unicast packets only, discard multicast and broadcast) and *multicast* (receive multicast and broadcast only, discard unicast packets).

Examples :

```
iwconfig eth0 power period 2
iwconfig eth0 power 500m unicast
iwconfig eth0 power timeout 300u all
iwconfig eth0 power off
iwconfig eth0 power min period 2 power max period 4
```

txpower

For cards supporting multiple transmit powers, sets the transmit power in dBm. If W is the power in Watt, the power in dBm is $P = 30 + 10 \cdot \log(W)$. If the value is postfixed by *mW*, it will be

automatically converted to dBm.

In addition, *on* and *off* enable and disable the radio, and *auto* and *fixed* enable and disable power control (if those features are available).

Examples :

```
iwconfig eth0 txpower 15
iwconfig eth0 txpower 30mW
iwconfig eth0 txpower auto
iwconfig eth0 txpower off
```

retry Most cards have MAC retransmissions, and some allow to set the behaviour of the retry mechanism.

To set the maximum number of retries, enter *limit value* . This is an absolute value (without unit). To set the maximum length of time the MAC should retry, enter *lifetime value* . By defaults, this value is in seconds, append the suffix *m* or *u* to specify values in milliseconds or microseconds.

You can also add the *min* and *max* modifiers. If the card supports automatic mode, they define the bounds of the limit or lifetime. Some other cards define different values depending on packet size, for example in 802.11 *min limit* is the short retry limit (non RTS/CTS packets).

Examples :

```
iwconfig eth0 retry 16
iwconfig eth0 retry lifetime 300m
iwconfig eth0 retry min limit 8
```

commit Some cards may not apply changes done through Wireless Extensions immediately (they may wait to aggregate the changes or apply it only when the card is brought up via *ifconfig*). This command (when available) forces the card to apply all pending changes.

This is normally not needed, because the card will eventually apply the changes, but can be useful for debugging.

DISPLAY

For each device which supports wireless extensions, *iwconfig* will display the name of the **MAC protocol** used (name of device for proprietary protocols), the **ESSID** (Network Name), the **NWID**, the **frequency** (or channel), the **sensitivity**, the **mode** of operation, the **Access Point** address, the **bit-rate**, the **RTS threshold**, the **fragmentation threshold**, the **encryption key** and the **power management** settings (depending on availability).

The parameters displayed have the same meaning and values as the parameters you can set, please refer to the previous part for a detailed explanation of them.

Some parameters are only displayed in short/abbreviated form (such as encryption). You may use **iwlist(8)** to get all the details.

Some parameters have two modes (such as bitrate). If the value is prefixed by '=', it means that the parameter is fixed and forced to that value, if it is prefixed by ':', the parameter is in automatic mode and the current value is shown (and may change).

Access Point/Cell

An address equal to 00:00:00:00:00:00 means that the card failed to associate with an Access Point (most likely a configuration issue). The **Access Point** parameter will be shown as **Cell** in ad-hoc mode (for obvious reasons), but otherwise works the same.

If */proc/net/wireless* exists, *iwconfig* will also display its content.

Note that those values will depend on the driver and the hardware specifics, so you need to refer to your driver documentation for proper interpretation of those values.

Link quality

Overall quality of the link. May be based on the level of contention or interference, the bit or frame error rate, how good the received signal is, some timing synchronisation, or other

hardware metric. This is an aggregate value, and depends totally on the driver and hardware.

Signal level

Received signal strength (RSSI - how strong the received signal is). May be arbitrary units or dBm, *iwconfig* uses driver meta information to interpret the raw value given by */proc/net/wireless* and display the proper unit or maximum value (using 8 bit arithmetic). In *Ad-Hoc* mode, this may be undefined and you should use *iwspy*.

Noise level

Background noise level (when no packet is transmitted). Similar comments as for **Signal level**.

Rx invalid nwid

Number of packets received with a different NWID or ESSID. Used to detect configuration problems or adjacent network existence (on the same frequency).

Rx invalid crypt

Number of packets that the hardware was unable to decrypt. This can be used to detect invalid encryption settings.

Rx invalid frag

Number of packets for which the hardware was not able to properly re-assemble the link layer fragments (most likely one was missing).

Tx excessive retries

Number of packets that the hardware failed to deliver. Most MAC protocols will retry the packet a number of times before giving up.

Invalid misc

Other packets lost in relation with specific wireless operations.

Missed beacon

Number of periodic beacons from the Cell or the Access Point we have missed. Beacons are sent at regular intervals to maintain the cell coordination, failure to receive them usually indicates that the card is out of range.

NAME

iwlist - Get more detailed wireless information from a wireless interface

SYNOPSIS

iwlist *interface* **scanning**

iwlist *interface* **frequency**

iwlist *interface* **rate**

iwlist *interface* **key**

iwlist *interface* **power**

iwlist *interface* **txpower**

iwlist *interface* **retry**

iwlist *interface* **event**

iwlist **--help**

iwlist **--version**

DESCRIPTION

Iwlist is used to display some additional information from a wireless network interface that is not displayed by **iwconfig(8)**. The main argument is used to select a category of information, **iwlist** displays in detailed form all information related to this category, including information already shown by **iwconfig(8)**.

PARAMETERS

scan[ning]

Give the list of Access Points and Ad-Hoc cells in range, and optionally a whole bunch of information about them (ESSID, Quality, Frequency, Mode...). The type of information returned depends on what the card supports.

Triggering scanning is a privileged operation (*root* only) and normal users can only read left-over scan results. By default, the way scanning is done (the scope of the scan) will be impacted by the current setting of the driver. Also, this command is supposed to take extra arguments to control the scanning behaviour, but this is currently not implemented.

freq[ueency]/channel

Give the list of available frequencies in the device and the number of defined channels. Please note that usually the driver returns the total number of channels and only the frequencies available in the present locale, so there is no one-to-one mapping between frequencies displayed and channel numbers.

rate/bit[rate]

List the bit-rates supported by the device.

key/enc[ryption]

List the encryption key sizes supported and display all the encryption keys available in the device.

power List the various Power Management attributes and modes of the device.

txpower

List the various Transmit Powers available on the device.

retry List the transmit retry limits and retry lifetime on the device.

ap/accesspoint/peers

Give the list of Access Points in range, and optionally the quality of link to them. This feature is **obsolete** and now deprecated in favor of scanning support (above), and most drivers don't support it.

Some drivers may use this command to return a specific list of Peers or Access Points, such as the list of Peers associated/registered with the card. See your driver documentation for details.

event List the wireless events supported by the device.

--version

Display the version of the tools, as well as the recommended and current Wireless Extensions version for the tool and the various wireless interfaces.

APÈNDIX B: Article “Insurrección Wireless”

Text extret d'una conferència impartida per l'advocat Carlos Sánchez Almeida al Novembre del 2004.

"Compartir la conexión a Internet con el vecino no debería ser considerado delito, sino únicamente un incumplimiento civil de contrato, un contrato que por otra parte es claramente abusivo: si se contrata un ancho de banda permanente, su utilización debería ser decidida por el usuario, y no por la empresa de telecomunicaciones.

La legislación represiva tiene un efecto perverso: estimula la imaginación, nos obliga a pensar distintas posibilidades de la tecnología. Como dijo John Gilmore, Internet siempre reacciona frente a la censura como un cuerpo orgánico, buscando alternativas para evitar la infección. Cuando me di cuenta de por dónde iban los tiros, empecé a darle vueltas a las posibilidades de la tecnología inalámbrica para eludir la represión. Hoy puedo decir que gracias al brazo tonto de la Ley, disponemos del argumento definitivo de la defensa. Como han tenido ocasión de comprobar los amigos que me visitan, la hospitalidad de mi casa no se limita a una copa de brandy. Si tengo conexión permanente a Internet, es un desperdicio no usarla. Si me sobra ancho de banda, que lo disfrute el amigo, o el vecino. Dejar la conexión wi-fi abierta es todo un detalle de urbanidad, que además cumple una función revolucionaria: hace inútil cualquier investigación policial basada exclusivamente en la IP.

Si una conexión wi-fi está permanentemente abierta, es imposible demostrar la procedencia de cualquier transmisión basada en esa IP, que puede tener su origen en cualquier ordenador situado en un rango de cien metros. Si multiplicamos esas conexiones abiertas a lo largo y ancho de la ciudad, el efecto expansivo es revolucionario. Sin orden de entrada y registro, una simple IP no prueba nada. Señores parlamentarios, muchas gracias: han conseguido socializar mis delitos. Compartir siempre es bueno: ha llegado el momento de la insurrección wireless."