# TREBALL DE RECERCA

## TECNOLOGIES SENSE FILS

## EL BLUETOOTH I LA WI-FI

# ÍNDEX DEL TREBALL

# INTRODUCCIÓ

La tecnologia sense fils realment ha arribat per quedar-se. S'ha anat convertint de mica en mica en la solució de molts problemes i incomoditats que representen tants cables. No només estèticament resulten incòmodes, sinó també en qüestions de treball.

Un dels productes més coneguts i possiblement els més utilitzats fins ara són els PDA (assistents personals de mà) que han anat impulsant el desenvolupament de les xarxes sense fils. Aquestes xarxes funcionen a base de transmissions infraroges o radiofreqüències que les uneixen amb els dispositius portàtils.

Tanmateix, les senyals infraroges només funcionen dins d'una mateixa habitació i cal que entre emissor i receptor es puguin veure i no hi hagi obstacles importants o parets, però les radiofreqüències funcionen normalment a través de qualsevol paret. Això és interessant i convenient ja que per exemple, a una oficina pot necessitar-se compartir informació dins del mateix espai (habitació/oficina), per aquest fi es pot utilitzar una xarxa sense cables infraroja, ningú s'entrebanca ni queda malament estèticament. Pel mateix, si es necessita que la informació es transmeti a un altre habitació, les xarxes per radiofreqüència són una gran opció per solucionar el problema.

Una cosa és indiscutible, aquest tipus de tecnologia està de moda i es troba present a la majoria dels dispositius electrònics del mercat. En aquest treball tractarem dos tipus de xarxa per radiofreqüència molt populars: el Bluetooth i la Wi-Fi, dels quals no sempre s'entenen les diferències i l'ús més apropiat per treure profit d'elles.

# CONCEPTES PREVIS

Actualment la ciència i la tecnologia avancen molt ràpidament i per entendre els nous medis de comunicació fa falta saber paraules noves, a vegades una mica difícils però que tenen la seva raó de ser. Per exemple, no podem parlar d'electrònica sense conèixer el transistor, o d'informàtica sense conèixer el bit i el byte.

El següent treball tracta en gran part el tema informàtic i la radiofreqüència. Començarem doncs amb les definicions de bit i byte:

- **Bit** és l'acrònim de Binary Digit (Dígit Binari). Un bit és un dígit del sistema de numeració binari. Mentre que al nostre sistema de numeració decimal utilitzem deu dígits, al binari s'utilitzen només dos dígits, el zero i l'u.

  El bit és la unitat mínima d'informació emprada a la informàtica, a qualsevol dispositiu digital, o a la teoria de la informació. Amb ell, podem representar valors qualsevol, com verdader o fals, obert o tancat, blanc o negre, nord o sur, masculí o femení...

- En català podem utilitzar **byte** o **octet**. Octet significa 8 bits. De fet, un byte s'ha de considerar com una seqüència de bits contigus, la mida dels quals depèn del codi d'informació o del codi de caràcters. Normalment s'utilitza com a unitat bàsica d'emmagatzemament d'informació combinant-la amb prefixos de quantitat.

  Els prefixos kilo, mega, giga... es consideren potències de 1024 en comptes de potències de 1000. Això és perquè 1024 és la potència de 2 ($2^{10}$) més propera a 1000. S'utilitza una potència de dos perquè la computadora treballa en un sistema binari.

La freqüència i la radiofreqüència són molt importants quan parlem de telecomunicacions. És necessari doncs fer una repassada als seus significats:

- La **freqüència** és una mesura que indica el número de repeticions de qualsevol fenomen periòdic per unitat de temps. Segons el SI (Sistema Internacional), el resultat es mesura en hertz (Hz), que representa un cicle per segon.

| | | | |
|---|---|---|---|
| 1 kilohertz | kHz | $10^3$ Hz | 1,000 Hz |
| 1 megahertz | MHz | $10^6$ Hz | 1,000,000 Hz |
| 1 gigahertz | GHz | $10^9$ Hz | 1,000,000,000 Hz |
| 1 terahertz | THz | $10^{12}$ Hz | 1,000,000,000,000 Hz |
| 1 petahertz | PHz | $10^{15}$ Hz | 1,000,000,000,000,000 Hz |
| 1 exahertz | EHz | $10^{18}$ Hz | 1,000,000,000,000,000,000 Hz |

- L'**espectre electromagnètic** és el conjunt de totes les possibles ones electromagnètiques, des de les de major freqüència, com els raigs gamma y raigs X, fins a les de menor freqüència, com les ones de ràdio. Evidentment les fronteres entre denominacions són convencionals i l'única diferència entre elles és la freqüència (o equivalentment, la longitud d'ona).

- La **radiofreqüència** és la part de l'espectre electromagnètic en què les ones electromagnètiques es poden generar mitjançant corrent altern aplicat a una antena i tradicionalment s'han utilitzat per a la comunicació. Tota aquesta banda de freqüències molt extensa, va des d'aproximadament els 3 Hz fins als 300 GHz.

I per acabar els conceptes previs és important esmentar els estàndards i el procés de normalització:

- A tecnologia i altres camps, un **estàndard** és una especificació d'alguns processos que regulen la fabricació de components, per garantir l'operativitat dintre de la societat. És l'objectiu de la normalització.

- La **normalització** es el procés d'elaboració, aplicació i millora de les normes que s'apliquen a les diferents activitats científiques, industrials o econòmiques a fi d'ordenar-les i millorar-les. Persegueix tres objectius fonamentals:

- Simplificar: Es tracta de reduir els models quedant-se només amb els més necessaris.
- Unificar: Per permetre l'intercanvi a nivell internacional.
- Especificar: Evitar els errors d'identificació creant un llenguatge clar i precís.

La proba que demostra la importància d'aquest fenomen, són tots els diners que inverteixen els països en desenvolupar organismes normalitzadors. A Espanya tenim la "Asociación Española de Normalización i Certificación", la web de la qual és http://www.aenor.es/.

# EL BLUETOOTH

## HISTÒRIA I FUTUR

El nom de la tecnologia Bluetooth es va prendre d'un rei danès del segle X anomenat Harald Blåtand (Harold Bluetooth en anglès), la traducció del qual és «dent blava», famós per les seves habilitats comunicatives i sobre tot per iniciar el procés de cristianització de la societat vikinga.

Pel que fa a la curta història d'aquesta tecnologia, els seus inicis daten de l'any 1994, quan la companyia Ericsson Mobile Communications va promoure una iniciativa per estudiar un entorn per radio entre els telèfons mòbils i els seus accessoris, amb la característica i condició d'un baix cost i consum. Fins llavors les tecnologies de comunicació basades en el cable funcionaven amb eficiència, tanmateix eren difícils o enrevessades d'instal·lar i configurar.

En aquell moment ja es trobava al mercat una tecnologia sense fils, els infrarojos, però aspectes com la seva velocitat de transmissió o la seva operativitat (els dispositius han de tenir línia visual entre ells) no han permès la seva expansió al mercat. Va ser llavors, quan es va arribar a la següent conclusió: una solució d'accés per ràdio a baix cost podia obrir un concepte absolutament nou, permetre la connexió entre dispositius sense cables i sense la necessitat d'haver línia visual entre emissor i receptor, inclús sense la necessitat d'estar a la mateixa habitació.

Però per a que el projecte arribés a bon port era necessari assegurar un estàndard estricte, que es popularitzés el seu ús i proporcionés als fabricants un model per desenvolupar productes amb aquesta tecnologia.

Per aconseguir un número suficient d'usuaris potencials i promocionar un únic estàndard mundial, Ericsson va establir relacions amb altres fabricants de dispositius mòbils durant 1997, i a principis de l'any següent es va constituir el SIG (Bluetooth Special Interest Group).

Aquest grup era format per Nokia, IBM, Toshiba, Intel i pels pioners d'Ericsson. El nou concepte de comunicació va rebre una excel·lent acollida i ràpidament es van anar unint membres al SIG, com ara les companyies 3COM, Compaq, Dell, Motorola, Lucent Technologies i la recentment adquirida per Intel, Xircom entre altres. Aquestes companyies, al ser participes del SIG, van poder proporcionar Bluetooth als seus productes amb la garantia que oferia el pertànyer al grup i conèixer les especificacions tècniques, a més de poder utilitzar lliurement la freqüència de radio del Bluetooth (2,4 Ghz), mentre que les companyies externes no podien aplicar-la al no tenir la seva patent.

El SIG va anar creixent fins arribar a més de 1800 membres a l'abril del 2000 i continua creixent avui en dia. Això significa que és una tecnologia pròspera amb molt per donar.

El futur del Bluetooth és prometedor. Degut a la similitud de les aplicacions entre Bluetooth i els infrarojos (els dos protocols especifiquen comunicació sense fils a curta distància), es creu que Bluetooth pot arribar a substituir-los.

Les següents característiques ens demostren els avantatges del Bluetooth envers els infrarojos:

- Els infrarojos requereixen comunicació lineal entre transmissor i receptor, el que fa imprescindible la línia de visió per a la seva transmissió.
- Les freqüències d'infraroig no permeten la penetració a través de les parets, el que representa un clar desavantatge contra el Bluetooth que si ho permet.
- La comunicació infraroja sempre es dona entre dos dispositius.
- Bluetooth permet la creació de xarxes.

# CARACTERÍSTIQUES GENERALS

- El Bluetooth és una **tecnologia sense fils** que actua a distàncies de fins a 10 metres amb velocitats d'un Mbps.

- L'estructura dels protocols que formen el Bluetooth afavoreix la **comunicació automàtica** sense necessitat de que el usuari l'inicii.

- La portabilitat i les petites dimensions dels dispositius requereixen un **baix consum** de potència.

- Els dispositius de comunicació que suporta poden experimentar un cost no major de 18 euros amb tendència a la baixa. A més, la seva operativitat es dona en una banda de freqüències no llicenciada (2,4GHz), el que afavoreix al seu **baix cost**.

- Bluetooth integra **serveis de transmissió** de veu i dades simultània.

- Degut a que basa la seva comunicació en la radiofreqüència (**transmissió omnidireccional)**, no requereix visió lineal entre dispositius i permet configuracions multi punt.

- Gràcies al **sistema de seguretat** Spread Spectrum Frequency Hopping, disminueix els riscos de que les comunicacions siguin interceptades o presentin interferències amb altres aplicacions. Proveeix també especificacions per autenticar dispositius que intenten connectar-se a la xarxa Bluetooth, així com un xifrat a les claus per protegir la informació.

- Per últim permet l'**establiment de xarxe**s. Té la característica de formar xarxes on un dispositiu fa de mestre i fins a set actuen com esclaus. Aquesta configuració es coneix com "piconet". Un grup de "piconets", de fins a deu, s'anomena Scatternet.

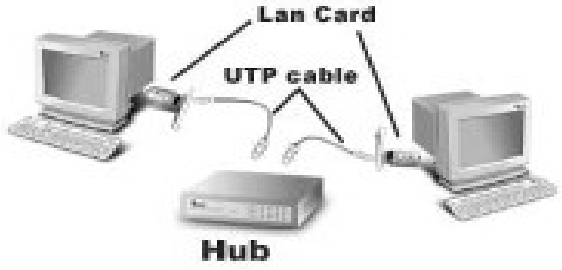
# LES XARXES LOCALS

Ara que ja coneixem el Bluetooth anem a continuar amb l'altre mètode de comunicació del treball, la Wi-Fi. Però no es pot explicar sense deixar clars uns conceptes bàsics, ja que Wi-Fi no serveix pel mateix que el Bluetooth.

Resumint molt per sobre podem afirmar que la Wi-Fi serveix per crear xarxes locals sense fils o WLAN.

# LES XARXES LAN

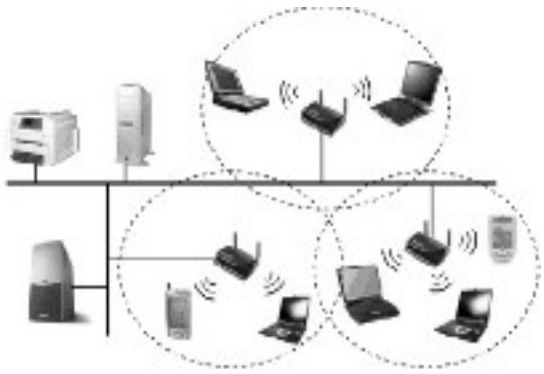
**LAN** és l'abreviatura de "Local Area Network" (Xarxa d'Àrea Local o simplement Xarxa Local). Una xarxa és la interconnexió d'alguns ordinadors i perifèrics. La seva extensió està limitada físicament a un edifici o a un entorn de pocs kilòmetres. Normalment s'utilitza per comunicar ordinadors personals i estacions de treball a oficines, fàbriques, a casa... per compartir recursos i intercanviar dades i aplicacions. En definitiva, permet que dues o més màquines es comuniquin. Aquesta connexió es fa mitjançant un cable de xarxa.




**Dibuix d'una xarxa LAN**

# LES XARXES WLAN

En aquest treball em centraré en les **WLAN**. WLAN és l'abreviatura de "Wireless Local Àrea Network" (Xarxa d'Àrea Local Sense Fils). Un sistema de comunicació de dades sense cables, molt utilitzat com alternativa a les xarxes LAN cablejades, o com a complement d'aquestes. Utilitza la tecnologia de la radiofreqüència, que permet més mobilitat als usuaris. Últimament, les WLAN estan adquirint molta importància en diversos camps, com ara magatzems o centrals de manufactura, on permeten comunicar la informació a temps real a la terminal de la central. No obstant, també són molt populars a les llars per compartir l'accés a Internet entre diverses computadores.



**Dibuix d'una xarxa WLAN**

# L'IEEE I L'ESTÀNDARD 802.11

## L'IEEE

IEEE són les sigles de l'Institut d'Enginyers Elèctrics i Electrònics "Institute of Electrical and Electronics Engineers", la major associació internacional sense afany de lucre formada per professionals de les noves tecnologies, enginyers elèctrics, electrònics, en sistemes i en telecomunicacions. Entre d'altres coses, es dediquen a la normalització. Amb el suport de més de 360.000 voluntaris de 175 països, l'IEEE és una autoritat amb màxim prestigi en les diferents àrees tècniques derivades de l'elèctrica original. Segons el mateix IEEE, el seu treball és promoure la creativitat, el desenvolupament i la integració, compartir i aplicar els avenços en les tecnologies de la informació, electrònica i ciències en general, per al benefici de la humanitat i dels mateixos professionals. L'estàndard IEEE 802.11 és un dels més importants, ja que governa l'especificació sense fils Wi-Fi.

## L'ESTÀNDARD IEEE 802.11

L'IEEE 802.11 és un estàndard de protocol de comunicacions de l'IEEE que especifica les normes de funcionament d'una WLAN. En general, els protocols de la branca 802.x defineixen la tecnologia de xarxes d'àrea local. Aquest protocol determinava velocitats d'un a dos Mbps i treballava a una freqüència de 2,4 GHz. L'any 1999 va aparèixer una modificació per al protocol 802.11, el 802.11b, amb velocitats de 5 a 11 Mbps i que treballava a la mateixa freqüència. Més endavant es va crear el 802.11a, capaç d'arribar als 50 Mbps amb freqüència de 5 Ghz, però no va desenvolupar-se perquè era incompatible amb el 802.11b. Al final van incorporar un estàndard de velocitat de 50Mbps que era compatible amb el 802.11b, el 802.11g.

Avui en dia la majoria de productes son de les especificacions b i g. Hi ha un problema, les xarxes que treballen sota els estàndards 802.11b i 802.11g poden sofrir interferències per part

dels microones, telèfons mòbils i altres equips que utilitzen la mateixa freqüència de 2,4 Ghz.

# LA WI-FI

# HISTORIA

L'origen de la Wi-Fi es remunta a la publicació en 1979 dels resultats d'un experiment realitzat per enginyers d'IBM a Suïssa, que va consistir en utilitzar enllaços infrarojos per crear una xarxa local a una fàbrica. Aquests resultats, publicats per l'IEEE, poden considerar-se com el punt de partida en la línia evolutiva de la Wi-Fi.

Les investigacions de les ones infraroges i de microones van seguir endavant, i al final, al maig de 1985, després de quatre anys d'intensos estudis, l'Agència Federal del Govern dels Estats Units, encarregada de regular i administrar les telecomunicacions, va assignar les bandes ISM (Industrial, Scientific and Medical – Industrial, Científica i Mèdica) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz, per a l´ús de les xarxes sense fils. Aquestes freqüències resultaven ideals per a la comunicació de dades, ja que eren molt poc susceptibles al soroll i creaven molt poques interferències.

L'assignació d'aquesta banda de freqüències va propiciar una major activitat industrial, i en aquest aspecte, les WLAN van començar a deixar l'entorn dels laboratoris per obrir-se camí cap al mercat comú.

Des de 1985 fins al 1990 es va seguir treballant, ja més en la fase de desenvolupament, fins que al maig de 1991 es van publicar diversos treballs referents a WLAN operatives que superaven la velocitat d'1 Mbps, el mínim establert per l'IEEE 802 per a que la xarxa sigués considerada realment una LAN, amb aplicació empresarial.

La Wi-Fi és un conjunt d'estàndards per a xarxes sense fils basats en les especificacions del IEEE 802.11. Es va crear per ser utilitzada en xarxes locals, però en l'actualitat el seu ús és més freqüent per accedir a Internet.

# CARACTERÍSTIQUES

Wi-Fi significa Wireless Fidelity (fidelitat sense fils) i és una marca registrada de la Wi-Fi Alliance, l'organització comercial que prova i certifica que els equips compleixin els estàndards del IEEE 802.11x.

Hi ha almenys tres tipus de Wi-Fi, cadascun basat en un estàndard de l'IEEE 802.11:

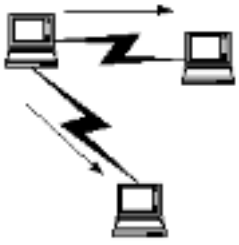
- L'estàndard 802.11 va ser el primer en aparèixer, té una velocitat de 2 Mbps i treballa a la banda de 2,4 GHz o dins de l'espectre infraroig.

- Els estàndards IEEE 802.11b i IEEE 802.11g, disposen d'acceptació internacional, ja que la freqüència 2,4 GHz es troba disponible quasi universalment, amb una velocitat de fins a 11 Mbps i 54 Mbps, respectivament. També existeix el IEEE 802.11n que treballa a 108 Mbps, encara que aquesta velocitat es possible d'obtenir amb l'estàndard 802.11g gràcies a unes tècniques d'accelerament que aconseguixen duplicar la transferència.

- Als Estats Units i Japó, s'utilitza també l'estàndard IEEE 802.11a, conegut com WIFI 5, opera a 5 Ghz, ofereix 54 Mbps i gaudeix d'una operativitat amb canals pràcticament nets. En altres zones com la Unió Europea, el 802.11a encara no està aprovat.

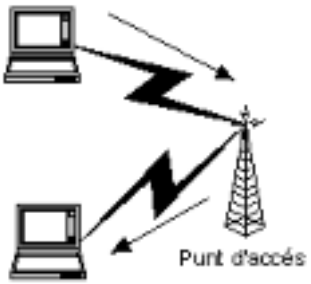
D'altra banda les xarxes locals sense fils es poden configurar de dues maneres bàsiques:

- En **mode *ad hoc*** (també anomenat peer-to-peer) al qual, cada màquina es pot comunicar directament amb la resta, però només amb les que estiguin dins de la seva zona d'abast.



**Exemple de mode *ad hoc***

- En **mode infraestructura:** S'instal·len punts d'accés als quals cada component de la xarxa sense fils envia la informació que es vol transmetre, aquest s'encarrega de distribuir-ho a tots els altres components de la xarxa. A la vegada, els punts d'accés permeten ampliar l'àrea de captació de la xarxa ( ja que efectuen com a repetidors) i també l'entrada de la informació a una xarxa cablejada ( poden actuar com a ponts). En aquest sentit no és una tecnologia substitutòria necessàriament, sinó que es pot fer servir per a donar un valor afegit a una xarxa existent en funcionament sense que s'hagi d'aturar per a posar-la en marxa.




**Exemple de mode infraestructura**

La comunicació entre els dispositius es basa en ones de ràdio o infraroges, tot i que aquestes últimes no són pràctiques per a moltes de les aplicacions de les WLAN. D'altra banda, les ones de ràdio es fonamenten en mecanismes desenvolupats per l'exèrcit, tal com sol passar en la major part dels avenços tecnològics (des d'Internet al microones). Aquesta tecnologia és coneguda com a espectre estès (Spread Spectrum) i es divideix en dos mecanismes diferents:

- En primer lloc tenim l'Espectre Estès de Salt de Freqüències (EESF): Sistema al qual l'emissor va saltant de freqüència en un patró que el receptor coneix. Es fa amb una correcta sincronització i es pot mantenir un sol canal lògic.

- L'altre és l'Espectre Estès de Seqüència Directa (EESD): Es genera un patró redundant per cada bit que s'ha de transmetre, anomenat xip, de manera que en cas de pèrdua d'informació aquesta pugui ser recuperada; amb això s'aconsegueix que sigui més resistent a qualsevol interferència.

Aquestes dues tecnologies son incompatibles entre elles, per tant s'ha d'estudiar quin emissor/receptor és més convenient en cada cas. Els aparells basats en l'EESF són més barats i consumeixen menys, però tenen menys zona d'abast que els EESD.

# EVOLUCIÓ I FUTUR

La preocupació per la seguretat va ser un dels problemes que més en compte van tenir les companyies des d'un principi, junt amb les restriccions pressupostaries. Poc a poc l'economia es va anar recuperant i es va anar treballant per millorar els nous estàndards en l'aspecte de la seguretat.

L'any 2002, el mercat de les solucions sense fils va arribar al seu punt més alt, movent uns 1.600 milions de dòlars. Any rere any el creixement ha sigut de més del 20%, tot i que encara hi ha nombrosos factors que frenen aquesta evolució, com la seguretat i la diversitat dels estàndards.

El futur de la Wi-Fi és bastant clar i prometedor. Actualment es pot parlar per telèfon utilitzant la xarxa Wi-Fi. Ja són quasi 40.000 punts al món els destinats a aquest camp i tot indica que continuaran creixent. La possibilitat de parlar per telèfon mitjançant la Wi-Fi es convertirà en una opció molt atractiva per a moltes de les majors cadenes hoteleres, i l'utilitzaran tant per als clients com per als treballadors d'aquestes.

Un exemple d'aquest servei de comunicació en expansió el representen els trens anglesos equipats amb punts Wi-Fi. Centenars de trens del Regne Unit portaran connexió a Internet amb Wi-Fi per als seus clients, gràcies a la combinació de les tecnologies de comunicació sense fils i la tercera generació de telefonia mòbil.

Els vagons d'aquests trens ja porten preses de corrent elèctric per a que els seus usuaris puguin connectar els seus equips informàtics i navegar per Internet. Les companyies Nomad Digital i Virgin  seran les encarregades d'equipar els trens britànics “West Coast” per proporcionar un servei continuu de 2Mbps.

Els experts argumenten que Wi-Fi i les tecnologies de consum relacionades són la clau per substituir les xarxes de telefonia mòbil.

De totes maneres, per a que això passi de forma internacional, encara falta molt de temps, ja que s'han de superar molts obstacles. Això no significa que no s'utilitzi, companyies com SocketIP o Symbol Technologies estan oferint plataformes telefòniques (substitució de centrals i terminals) que utilitzen el transport Wi-Fi.

D'altra banda, el diari EL PAÍS publicava el passat 8 de gener una notícia que toca de ple el meu treball. Segons l'article, la ciutat de San Francisco i l'empresa EarthLink han arribat a un acord provisional per oferir accés a Internet gratuït i sense fils, amb l'objectiu de convertir-se en la primera ciutat dels EEUU que proporciona un servei municipal de Wi-Fi a tot el seu territori.

Potser és aquest el principi d'una nova era de la informació gratuïta? Ja ho veurem amb el temps.

# ELS SISTEMES DE SEGURETAT

Tanmateix, un dels problemes més greus als quals s'enfronta actualment aquesta tecnologia, és la seguretat. Moltes de les xarxes són simples d'instal·lar i configurar, el que porta a l'usuari novell a instal·lar-les sense considerar la seguretat i, per tant, converteixen la seva xarxa en oberta sense protegir la informació que circula per elles.

Existeixen diverses alternatives per garantir la seguretat de les xarxes. Les més comuns són la utilització dels protocols de seguretat de dades específiques, com el WEP i el WPA, que s'encarreguen del següent:

- Autenticar: Procés pel qual l'usuari s'identifica d'una forma unívoca i en molts casos sense la possibilitat de rebutjar-la. Una vegada identificat, l'usuari podrà accedir a determinats recursos del sistema.

- Integrar: Adaptar la informació al sistema.

- "Confidenciar": Fer confidencial la informació de manera que únicament pugui accedir l'usuari identificat.

La majoria d'aquests protocols són proporcionats pels mateixos dispositius sense fils.

En l'actualitat, el millor protocol de seguretat Wi-Fi és l'anomenat WPA2, una millora relativa del WPA. Per poder utilitzar-lo s'ha de disposar d'un ordinador amb Windows XP amb el Service Pack 2 i una actualització addicional.

# EL SISTEMA WEP

L'estàndard 802.11 defineix un sistema per l'autenticat i xifrat de les comunicacions WLAN que es diu WEP (Wireless Equivalent Privacy). WEP requereix una paraula clau que serà utilitzada per autenticar-se en les xarxes WEP tancades i per xifrar els missatges de la comunicació.

Per generar aquesta clau, molts AP (Acces Point) demanen una frase i després, a partir d'ella, generen 5 claus diferents per garantir el màxim d'atzar en l'elecció de la mateixa. D'altres simplement demanen una clau, respectant les restriccions de longitud per configurar-les.

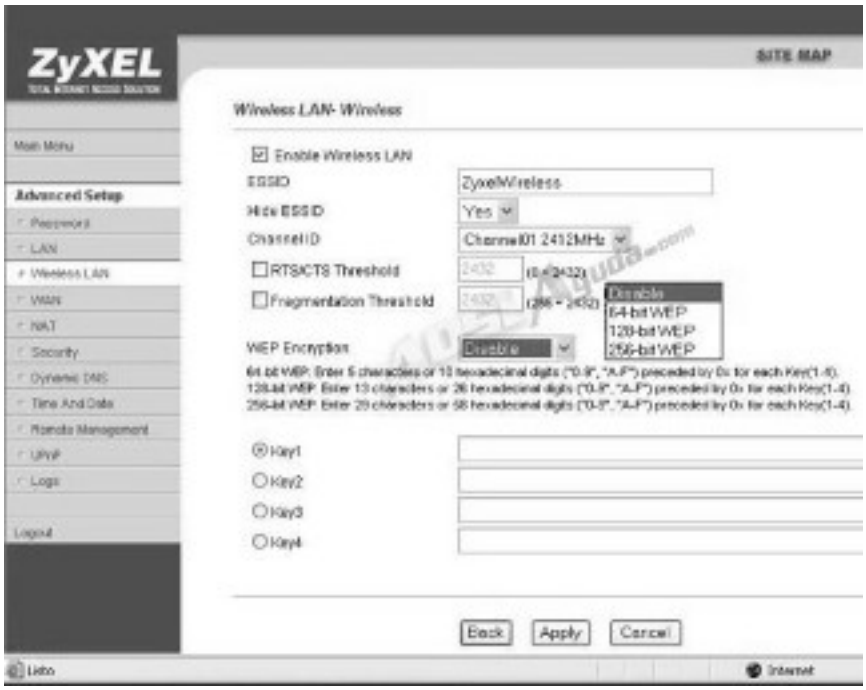
Per al xifrat de cada tram s'afegirà una seqüència canviant de bits, anomenats Vectors d'Inicialització (IV), amb l'objectiu de no utilitzar sempre la mateixa clau de xifrat i desxifrat.

Normalment, quan configurem una connexió sense fils, el mateix "mòdem - router" ens preguntarà quin tipus de xifrat volem, de 64, 128 o fins i tot 256 bits.

Quan ens referim a "tants" bits, en realitat parlem de lletres o números en la nostra clau. Òbviament, quan més llarga sigui la clau, més volum de bits ocuparà:

- Per a 64 bits: 5 Caràcters o 10 dígits hexadecimals ("0 a 9" "A a F" precedits per "0x", on x un dígit de l'1 al 4)
- Per a 128 bits: 13 Caràcters o 26 dígits hexadecimals ("0 a 9" "A a F" precedits per "0x", on x un dígit de l'1 al 4)
- Per a 256 bits: 29 caràcters o 58 dígits hexadecimals ("0 a 9" "A a F" precedits per "0x", on x un dígit de l'1 al 4)

Fixem-nos en la fotografia:




**Exemple de configuració d'un Router Wi-Fi Zyxel 660**

No obstant, aquest protocol de xifrat té molts defectes. El principal problema es troba amb la mida dels vectors d'inicialització. La quantitat de trames que passen a través d'un punt d'accés és molt gran, el que fa que ràpidament es trobin dos missatges amb el mateix vector d'inicialització i per tant sigui fàcil fer-se amb la clau. Aquest sistema és insegur degut a la seva implementació, ja que augmentar la mida de les claus només augmentaria el temps necessari per desxifrar-les.

Per "crackejar" (introduir-se) a una xarxa solen utilitzar-se els denominats Packet Sniffers i els WEP Crackers. Tots aquests programes es poden trobar a Internet sense gran dificultat, i

gràcies a l'existència de guies penjades a molts fòrums, fins i tot algú que no té ni idea pot introduir-se en una WLAN...

El procés és més o menys el següent:

Es captura la quantitat necessària de paquets (dependrà del codi de xifrat) mitjançant la utilització d'un Packet Sniffer, i després utilitzant un WEP Cracker o Key Cracker, es tractarà de trencar el xifrat de la xarxa. Els Key Crackers són uns programes basats en l'enginyeria inversa, en comptes de xifrar els paquets els desxifren.

Llavors, per què si és tan vulnerable és el més popular i utilitzat? Per què no s'adopten altres tipus més segurs com el WPA? És fàcil d'explicar. WEP és senzill de configurar i qualsevol sistema amb l'estàndard 802.11 el suporta. Per contra, això no passa amb WPA. Molt hardware antic l'utilitza i el nou passa a utilitzar el nivell de seguretat anterior per poder ser compatible.

# EL SISTEMA WPA

El WPA (Wi-Fi Protected Acces - Accés Protegit Wi-Fi ), és un sistema creat per l'Aliança Wi-Fi amb l'objectiu de protegir les xarxes sense fils i corregir les deficiències del sistema WEP. La informació també es xifra utilitzant una clau de 128 bits, ja que WPA no elimina el procés de xifrat WEP, sinó que l'enforteix.

Incrementant la mida de les claus i afegint un sistema de verificació de missatges, WPA fa que l'entrada no autoritzada a les xarxes sigui molt més difícil. Els dissenyadors van crear i implantar l'algoritme més fort possible, el Michael. Tanmateix, aquest algoritme tenia que funcionar a les targetes de xarxa sense fils més velles, i això, era un risc a ser atacat. Per

eliminar aquest problema, els dissenyadors van programar les xarxes WPA per desconnectar-se durant 60 segons al detectar dos intents d'atac en un minut.

# ELS PROBLEMES LEGALS DE LA WI-FI

Suposem per un moment que encenem el nostre portàtil quan estem asseguts al sofà i responem "Acceptar" a la pregunta de si volem accedir a un punt d'accés a Internet propietat del veí.

¿Quina responsabilitat potencial podria suposar-nos accedir al punt d'accés d'una xarxa Wireless que no és la nostra? Què passa si s'intercepten senyals d'una connexió sense fils? Què passa si configurem un punt d'accés insegur o obert a la nostra empresa o a casa nostra?

Hi ha una gran polèmica en aquest aspecte. Els advocats tindran que veure-se-les amb aquests problemes i altres relacionats si la tecnologia sense fils continua popularitzant-se.

¿Què passa actualment?

El contracte de subministrament d'ADSL inclou explícitament la clàusula de no redistribució a tercers. A més no es pot ser proveïdor d'accés a Internet sense permís de la CMT (Comissió del Mercat de les Telecomunicacions).

Pensem en el pobre pare, cap de família, que no sap configurar correctament l'ADSL Wi-Fi de Telefònica i subministra sense adonar-se connexió a tercers :

- Primerament està violant el contracte de subministrament del seu proveïdor.
- I en segon lloc està violant la Llei General de Telecomunicacions actuant com a proveïdor d'accessos.

Doncs bé, aquest home podria perfectament ser demandat pel proveïdor o demandar ell al proveïdor per haver-li donat un equip que per defecte ho deixa tot obert... per inducció al delicte.

En quant a la persona que roba la connexió, és un peix que es mossega la cua, ja que la LGT (Llei de General Telecomunicacions) diu que la recepció és lliure i una interpretació restrictiva de la LSSI (Llei de Serveis de la Societat de la Informació) podria qualificar com delicte d'estafa l'ús d'una connexió Wi-Fi aliena.

Tot plegat és el paradís dels advocats...

**Dibuix d'un home robant la xarxa Wi-Fi del seu veí**

# LA WI-FI COMERCIAL

De vegades, quan anem a una superfície comercial o d'oci podem trobar cartells que diuen: "En aquest local disposem de Wi-Fi al servei dels usuaris". Això significa que aquests establiments disposen d'una WLAN per a que els hostes puguin connectar-se a Internet mentre fan altres activitats, com ara beure un cafè. L'usuari només ha de disposar d'un ordinador portàtil amb receptor Wi-Fi integrat.

Segons una investigació duta a terme per ABI Research, companyia que assessora a fabricants de tot el món dels semiconductors sense fils, durant el passat any el número de punts Wi-Fi comercials va augmentar en un 47% a tot el món, fins arribar als 143.700.

Tot i que tres quartes parts d'aquests punts (el 74%) es troben repartits entre el nord d'Amèrica i Europa, el cert és que en la regió d'Àsia Pacífica el número augmenta molt ràpidament. Segons explica ABI Research al comunicat, l'any 2010 aquesta àrea del món superarà a Europa i Nord Amèrica en nombre de punts Wi-Fi.

En l'actualitat, la líder del mercat és Europa, amb més de 57.000. Un dels majors usuaris Wi-Fi són els establiments de menjar ràpid, com ara McDonalds, que n'ha instal·lat en un 17% dels seus 4.000 establiments.

El mercat a l'alça de punts Wi-Fi es percep en les xifres: més de 675.000 punts d'accés seran posats aquest any per aquest ús específic. I no només augmenten els usuaris i l'extensió, sinó també el número de sessions abonades, és a dir, que cada vegada els usuaris dediquen més temps a navegar per Internet i a utilitzar el correu electrònic.

Un altre estudi, dut a terme per BroadGroup, ha determinat que a Europa el número de punts d'accés va créixer un 28% entre maig del 2005 i setembre del 2006. Aquesta estudi representa 139 serveis a 28 països, el que representa més de 350 productes analitzats, la majoria d'ells centralitzats al Regne Unit, Alemanya i França.

En tot cas, actualment a Espanya no hi ha gaires, però d'aquí a pocs anys es posaran de moda i segurament podrem trobar bastants punts a les ciutats.

# MOVIMENT SOCIAL

## LES ORGANITZACIONS DE LA WI-FI LLIURE

Fa uns anys va aparèixer una tendència entre els usuaris de Wi-Fi, la d'experimentar amb les comunicacions i les radiocomunicacions, tot aprofitant la tecnologia de l'estàndard 802.11, que ofereix més oportunitats de les que sembla a simple vista. Aquesta tendència la segueixen centenars de grups i associacions de la Wi-Fi lliure repartides per les ciutats de tot el món.

Aquests grups es basen en el següent:

Mitjançant la instal·lació de punts d'accés repartits per les ciutats i la interconnexió d'aquests, es pot aconseguir crear una Xarxa d'Àrea Metropolitana (Metropolitan Area Network – MAN) i a la vegada proporcionar accés a aquesta xarxa i potser a Internet a tothom de manera lliure i a un baix cost.

Tanmateix, donar cobertura a una gran ciutat requereix molts punts d'accés i per tant molta gent disposada a oferir el servei i invertir una mica del seu temps i diners en la instal·lació i manteniment dels nodes i servidors. Aquest projecte tan gran i costós té una sèrie de problemes:

- Problemes tècnics: Instal·lació i manteniment del hardware i software necessari.
- Problemes econòmics: El hardware, l'electricitat i les connexions a Internet costen diners.
- Problemes legals: S'ha d'estudiar i complir amb la legislació vigent per a que els projectes tinguin futur.

La primera fase d'aquestes organitzacions és la de situar-se, saber on estan i amb quins punts

a favor i en contra conten. Quina tecnologia poden utilitzar i com, conèixer els productes dels fabricants del mercat del seu país i la compatibilitat entre ells, han d'estudiar els preus etc.

La segona fase és començar a pensar el que volen fer, buscar gent i intentar crear un projecte sòlid.

Però, poden muntar un moviment com aquest legalment? Què diu la llei al respecte? Aquests grups es defensen amb l'existència d'associacions similars als Estats Units i a Europa i d'una legislació comú Europea relacionada amb les comunicacions digitals i les xarxes privades, la CEPT.

Actualment hi ha organitzacions que donen suport als petits grups de xarxes lliures, com per exemple el projecte RedLibre, que dóna informació de com començar els projectes de Wi-Fi lliure i que pretén formar una gran xarxa espanyola.

# LA WI-FI LLIURE AL BAGES

Actualment la major part dels nodes o xarxes es troben a Manresa i són portats per l'associació Guifibages, formada en un principi per estudiants de la UPC i que conta amb el suport de l'ajuntament. Hi ha altres poblacions del Bages que disposen de Wifi lliure, com ara Callús o Sant Feliu Sasserra.

En un futur està prevista la construcció d'altres nodes en les localitats d'Artés, Navàs, Navarcles etc. En la següent taula, extreta de Guifi.net podem observar amb més detall l'estat dels nodes del Bages.

**NODES EL BAGES**

| Població | Funcionant | Projectats | En construcció | En proves | Total |
|---|---|---|---|---|---|
| Artés | 0 | 8 | 0 | 0 | 8 |
| Avinyó | 0 | 1 | 0 | 0 | 1 |
| Callús | 5 | 5 | 0 | 0 | 10 |
| Castellfollit del Boix | 0 | 3 | 0 | 0 | 3 |
| Estany, L' | 0 | 1 | 0 | 0 | 1 |
| Fonollosa | 0 | 1 | 0 | 0 | 1 |
| Manresa | 6 | 9 | 1 | 3 | 19 |
| Moià | 0 | 1 | 0 | 0 | 1 |
| Navarcles | 0 | 2 | 0 | 0 | 2 |
| Navàs | 0 | 6 | 1 | 0 | 7 |
| Sant Feliu Sasserra | 1 | 7 | 1 | 0 | 9 |
| Santa Maria d'Oló | 0 | 1 | 0 | 0 | 1 |
| St. Salvador de Guardiola | 0 | 1 | 0 | 0 | 1 |
| | **12** | **46** | **3** | **3** | **64** |

Com a conclusió de la taula podem dir que no tenim gaires punts funcionant, tot i que està previst quintuplicar els nodes. Hi ha una explicació bastant simple. Les organitzacions com ara Guifi.net estan progressant perquè hi ha molts interessats en el tema al seu territori, com ara ramaders que necessiten d'aquests serveis, o gent que no li arriba la connexió telefònica. Al Bages, la majoria d'associacions no compten amb gaire gent, i això tant si es vol com si no, impedeix el seu desenvolupament.

# OSONA I GUIFI.NET: ELS PRIMERS DEL MÓN

Potser no ho sembla, però Catalunya està molt activa en l'aspecte de Wi-Fi lliure. De fet, és aquí on es troba la major xarxa sense fills lliure del món, no universitària ni empresarial, a la qual es connecten més de 3.000 persones de forma gratuïta.

A la comarca d'Osona, ramaders, cases de turisme rural, associacions, empreses, particulars i ajuntaments estan units a través d'antenes instal·lades en llocs tan estranys com ara un dipòsit d'aigua municipal o un campanar del segle XII.

El grup de gent que es troba darrera d'aquests fets és Guifi.net. Van néixer a començaments de 2004 i avui en dia cobreixen un territori de 1.000 Km², mitjançant més de 1.000 nodes que connecten a unes 3.000 persones, 23 ajuntaments i inclús algun Seminari de Vic i la Casa Sacerdotal, tot plegat representa un tràfic anual de 1.000 Terabytes. Qualsevol pot accedir gratuïtament a aquesta xarxa, només fa falta una petita antena que val entre 200 a 300 euros.

Hi ha unes 20 persones voluntàries que porten el pes de l'organització tècnica. Ells són els encarregats de crear els programes necessaris, de parlar amb els veïns interessats, muntar els super nodes i ensenyar als usuaris com arreglar els possibles errors que puguin sorgir. A més a més compten amb la col·laboració esporàdica d'unes 200 persones.

El més sorprenent de tot això és el que explica el fundador de Guifi.net Ramon Roca:

"No som una associació, no rebem subvencions, no tenim ànim de lucre, la xarxa és de tots i de ningú. Qualsevol es pot implicar en el grau que vulgui. Si un node o punt de connexió cau i ningú va arreglar-lo, això vol dir que no se'l mereixen. Si és a prop de casa teva, vas. El primer que s'adona de l'error l'arregla."

Afegeix: "La clau de l'èxit de l'organització és que tot funciona gràcies als programes lliures i de gestió tècnica creats per nosaltres mateixos. El problema de les primeres xarxes d'aquest tipus va ser que no tenien programes per automatitzar la gestió i si creixien molt eren

immanejables".

Actualment, Guifi.net intenta ser un model universal que pretén ajudar a resoldre problemes amb aquestes xarxes arreu del món. De fet, les xarxes del Maresme, Vallès, Bages o de l'Anoia estan utilitzant la plataforma tècnica creada per Guifi.net.

És interessant comentar que aquesta xarxa no ofereix Internet. És una Intranet (xarxa LAN) on es pengen webs, serveis de Veu IP, radio o servidors. Però els usuaris que tenen Internet poden fer "autoprestació"de la seva connexió a nivell d'amic o públic en general. Cadascú decideix què i sota quines condicions.

Tanmateix, aquest projecte va tenir entrebancs en un principi. La desinformació de les institucions sobre les conseqüències legals d'oferir Internet van ser un problema per ells. Totes les institucions deien que era il·legal, però la CMT (Comissió del Mercat de les Telecomunicacions) mai a prohibit l'autoprestació. Per això el projecte va tirar endavant i segueix desenvolupant-se actualment.

# PRÀCTICA: MUNTAR I CONFIGURAR UNA WLAN

L'objectiu d'aquesta pràctica és explicar com muntar una xarxa sense fils de dos ordinadors, un de sobretaula i un portàtil, connectada a Internet sota Windows XP i amb un mínim de seguretat.

Imaginem-nos que fa un temps vam contractar l'ADSL de Telefònica i ens van proporcionar un Mòdem USB. Ara tenim un ordinador portàtil i volem posar Wi-Fi per connectar-nos als dos ordinadors. Òbviament amb el Mòdem USB és impossible fer-ho. Llavors, o tenim que demanar a Telefònica que ens el canvii i ens proporcioni un nou Mòdem-Router amb emissor Wi-Fi (ens cobrarà una pasta) o bé ens ho muntem pel nostre compte, comprant un hardware alternatiu i configurant-lo nosaltres mateixos.

La gent creu que configurar hardware alternatiu és molt més complicat que seguir els 4 passos del mòdem de Telefònica, però en realitat tampoc hi ha per tant. A mi em va passar i aprofitaré l'experiència per explicar com ho vaig fer.

# Pas 1: Recompte del hardware

– Òbviament un ordinador de sobretaula i un portàtil: Personalment disposo d'un AMD Athlon(tm) 64 Processor i un Sony VAIO Dual Core amb receptor Wi-Fi integrat.

– 1 router Linksys Wireless-G WAG54G ver.2.

– 1 Targeta de xarxa NVIDIA nForce Networking Controller (inclosa a la placa mare).

– 1 Cable de xarxa, 1 de telèfon i l'adaptador de corrent del router.

# Pas 2: Preparant l'ordinador

Ens situem a l'ordinador de sobretaula. Procedim a desinstal·lar tots els programes relacionats amb l'anterior Mòdem USB i reiniciem. Connectem el router apagat a la corrent, a la línia telefònica i a l'ordinador mitjançant el cable de xarxa. Després posem el router en funcionament i esperem a que Windows el detecti.

Normalment els routers no necessiten controladors addicionals per funcionar, en el cas que Windows no el detecti s'han d'instal·lar els drivers que normalment es troben a un CD que ve amb el router.

# Pas 3: Configurant la connexió a Internet

Una vegada connectat el router podem procedir a configurar-lo. Hi ha moltes pàgines web que ofereixen ajuda sobre com configurar els diferents models, només has de buscar el nom del teu router i seguir uns passos. En el meu cas tinc un router Linksys Wireless-G WAG54G i una connexió ADSL de Telefònica Dinàmica PPPoE:

Abans de tot farem un "reset" al router pressionant durant 10 segons el botó del darrera, això ho farem per si ve configurat, esborrarem així totes les dades per poder començar des de zero.

La direcció IP (Internet Protocol – Protocol d'Internet) per defecte del router és 192.168.1.1. Per poder connectar amb ell, en el cas de que no tinguem comunicació, haurem de configurar la nostra targeta de xarxa en el mateix nivell (192.168.1.xxx y màscara 255.255.255.0) o bé posant-la per a que obtingui una direcció IP automàticament, ja que el servidor DHCP (Dynamic Host Configuration Protocol – Protocol de Configuració del Servidor Dinàmic) del router ve activat. Això ho fem a la pantalla de propietats del protocol TCP/IP (Transmission Control Protocol – Protocol de Control de Transmissió) de la nostra targeta de xarxa.

Per tant, escriurem la direcció 192.168.1.1 a la barra de direccions de qualsevol navegador, i ens sortirà el següent missatge (en cas de donar error es tindrà que configurar la targeta de xarxa).


Les claus predeterminades d'accés al router són: **Usuari: admin. Contrasenya: admin.**

Una vegada ens hàgim identificat com administradors, la primera pantalla que ens apareixerà és la de configuració. Aquí és on tindrem que fer totes les operacions.

Els valors que haurem d'introduir en els diferents camps són els de la imatge superior (configuració tipus per a Telefònica). El significat dels paràmetres són els següents:

- **Encapsulation**: RFC 2516 PPP0E
- **Virtual Circuit**: VPI 8. VCI 32
- **Multiplexing**: LLC
- **Service Name**: Aquest camp és imprescindible que el deixem en blanc. En cas contrari no funcionarà la connexió a Internet.
- **User Name**: Nom d'usuari de la nostra connexió adsl. En el cas de Telefònica adslppp@telefonicanetpa.
- **Password**: Contrasenya de la connexió adsl. Per a Telefónica adslppp.
- **Connection**: Podem seleccionar qualsevol de les dues opcions. A la primera d'elles (Connect on Demand), el router es connectarà quan algun dels nostres PCs el demani, desactivant la connexió a Internet després de 5 minuts d'inactivitat. A la segona opció (Keep Alive), la connexió seguirà sempre activa.
- Els camps **Host Name** y **Domain Name** només s'ompliran si el nostre ISP ho requereix.

La segona part de la pantalla de configuració:


El valor **MTU** el deixem com està, en **Automatic**.

Tots els altres valors de la configuració pertanyen als valors de xarxa local, com direcció IP, Màscara "Subxarxa" i Servidor DHCP del router. No es necessari tocar-los per definir la connexió a Internet.

El que tenim que decidir es si volem teninr activat el servidor DHCP del router. Si està activat, el router proporcionarà una direcció IP automàticament als ordinadors que el sol·licitin. Si està desactivat, haurem de configurar manualment les targetes de xarxa de cadascun d'ells.

# Pas 4: Configurant la seguretat de la xarxa

Codificar la connexió sense fils és protegir-la mitjançant una clau, de manera que només els ordinadors amb la configuració que coincideixi amb el router tindran accés. És necessari per

mantenir la nostra xarxa davant dels intrusos, en el cas de xarxes domèstiques, poden ser molt sovint els nostres "estimats" veïns.

El procés consisteix en dos passos:

- Configurar la codificació al router.
- Configurar la codificació a la targeta de xarxa Wireless de cada ordinador.

El router suporta 2 tipus de codificació:

- WEP (*Wired Equivalent Privacy):* Ens ofereix dos nivells de seguretat, codificació a 64 o 128 bit. La codificació utilitza un sistema de claus. La clau de la targeta de xarxa de l'ordinador ha de coincidir amb la clau del router.
- WPA (*Wireless Protected Access*): Ofereix dos tipus de seguretat, amb servidor de seguretat i sense servidor. Aquest mètode es basa en tenir una clau compartida d'un mínim de 8 caràcters alfanumèrics per a tots els llocs de la xarxa (sense servidor) o disposar d'un canvi dinàmic de claus entre quests llocs (amb servidor). És una opció més segura, però no tots els dispositius Wireless la suporten.

Per accedir a la configuració de seguretat Wireless, haurem d'entrar a la configuració del router, tal i com hem fet al Pas 3.

Una vegada dintre escollim l'opció **Wireless Security**.


Apareixerà un desplegable on podrem escollir quatre opcions de seguretat o codificació:


Això significa que hi ha 4 opcions diferents per protegir la xarxa Wi-Fi, l'usuari pot escollir el tipus que vulgui, jo explicaré com configurar els quatre.

# 1: SISTEMA WEP

Tenim dues possibilitats de codificació WEP:

## A: WEP 64-bits

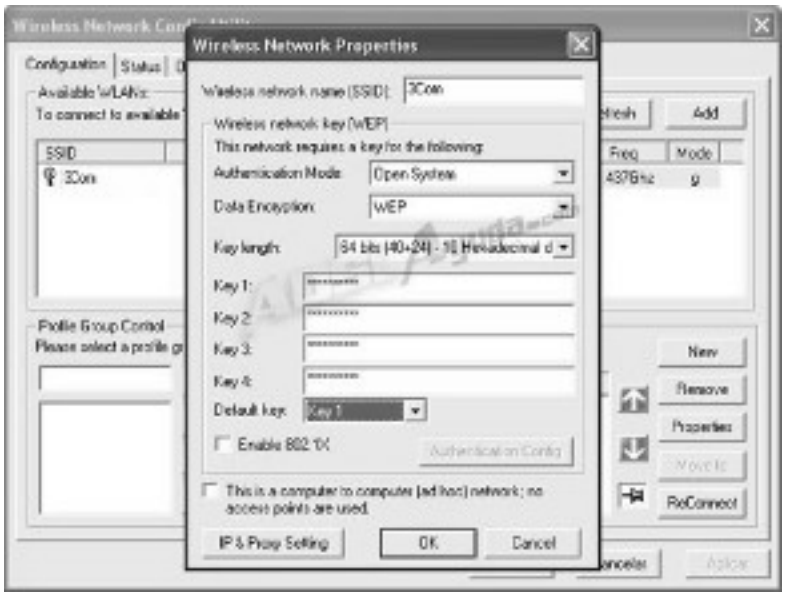
Al seleccionar-la, la pantalla canviarà per a que introduïm las claus:


Podem introduir manualment números hexadecimals a les caselles corresponents o bé utilitzar una frase de pas per a que el mateix router les generi.


Escriurem una frase i farem clic a **Generate**, llavors el router establirà les claus que més tard utilitzarem per a cada dispositiu Wireless que vulguem connectar. Aquestes claus haurem de

copiar-les i tenir-les a mà guardades. Per últim farem clic a **Save Settings**. Es produirà el procés de codificació de la transmissió sense fils i perdrem la connexió.

A continuació introduirem la mateixa clau al portàtil o als altres ordinadors que vulguem connectar. Això ho configurarem al software específic, o si tenim receptor integrat, al mateix programa que inclou Windows XP (millor amb el Service Pack 2).




**Configuració WEP 64-bit d'un receptor Conceptronic.**

Una vegada configurada la targeta, l'ordinador haurà de recuperar la connexió amb el router.

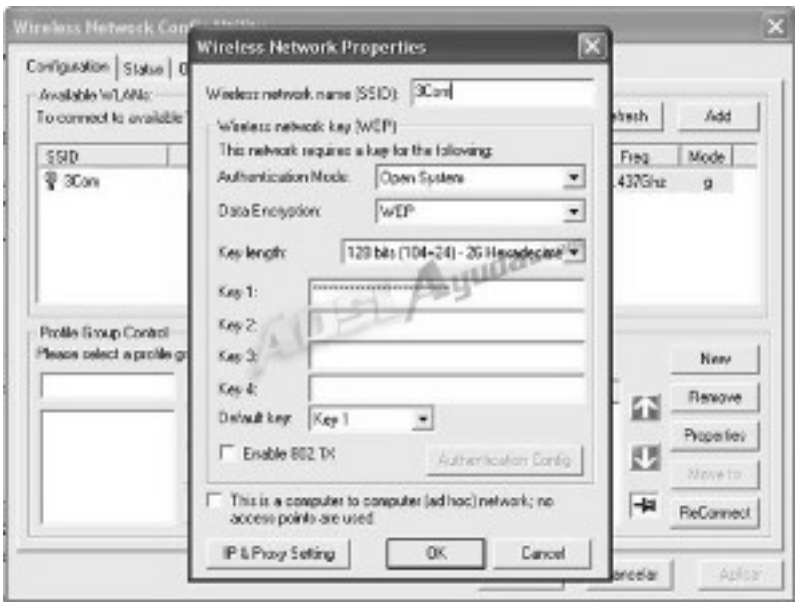
## B: WEP 128-bits

És un mètode semblant a l'anterior, utilitza una clau més llarga i per tant, se suposa que és més segur. La pantalla d'introducció de claus és diferent però l'us és el mateix.

Podem introduir manualment números hexadecimals a les caselles corresponents o utilitzar la frase de pas.


Escriurem la frase i farem clic a **Generate**, copiarem les claus per introduir-les a cada dispositiu Wireless que vulguem connectar. Per últim farem clic al botó **Save Settings**. Perdrem la connexió fins que configurem la descodificació als ordinadors amb el software específic de la targeta sense fils de cadascun.

Per exemple, amb la targeta del cas anterior:




**Configuració WEP 128-bit d'un receptor Conceptronic.**

Una vegada configurada la targeta, l'ordinador haurà de recuperar la connexió amb el router.

Segons Microsoft, únicament s'ha d'utilitzar el sistema obert/WEP si cap dispositiu de xarxa admet WPA. Per això es recomana utilitzar sempre que es pugui, dispositius sense fils compatibles amb WPA i WPA-PSK/TKIP.

## 2: SISTEMA WPA Pre-Shared Key

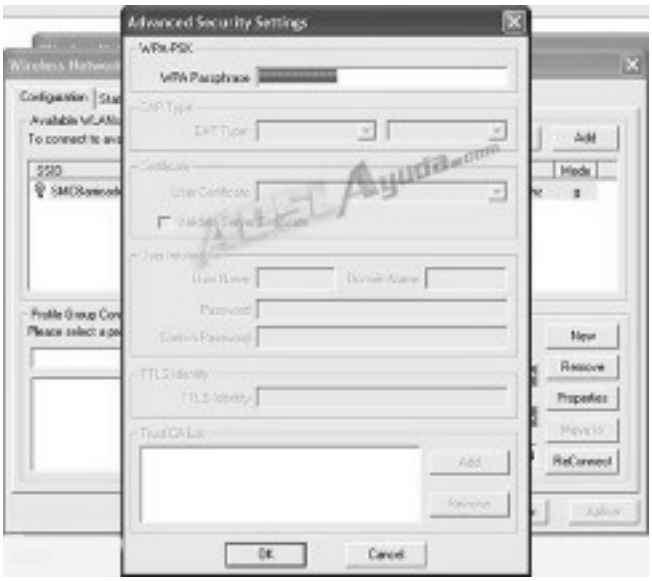
Tècnicament, WPA-PSK (Wi-Fi Protected Access Pre-Shared Key), significa "Accés protegit de fidelitat sense fils amb clau prèviament compartida". La codificació utilitza l'autenticació de clau prèviament compartida amb xifrat TKIP (Temporal Key Integrity Protocol - Protocol d'integritat de clau temporal), que es va denominar WPA-PSK/TKIP.

Segons la descripció de Microsoft, WPA-PSK proporciona una sòlida protecció mitjançant la codificació per als usuaris domèstics de dispositius sense fils. Per mitjà del procés TKIP, les claus de codificació canvien amb tanta rapidesa que un pirata informàtic és incapaç (això dependrà molt del pirata...) de reunir suficients dades amb la rapidesa necessària per

desxifrar el codi.

Per configurar-la, escollim al menú desplegable la opció corresponent:


Al camp **WPA Shared Key** escriurem la clau que vulguem assignar i l'haurem d'introduir també a tots els dispositius Wireless que vulguem connectar al router. Per últim farem clic a **Save Settings**. Perdrem la connexió fins que configurem la codificació als ordinadors amb el software específic de la targeta sense fils de cadascun. Per exemple, amb la targeta d'abans:



**Configuració WPA Pre-Shared Key d'un receptor Conceptronic.**

Una vegada configurada la targeta, l'ordinador recuperarà la connexió amb el router.

## 3: WPA (amb servidor RADIUS)

**RADIUS** significa Remote Authentication Dial-In User Service.

És un Sistema d'autenticació emprat habitualment per la majoria de proveïdors de serveis d'Internet (ISPs). Quan l'usuari realitza una connexió al seu ISP ha d'introduir el seu nom d'usuari i contrasenya, aquesta informació passa a un servidor RADIUS que verifica la informació i autoritza l'accés al sistema del ISP.


Els següents passos descriuen el plantejament genèric que s'utilitzaria per autenticar l'equip d'un usuari de mode que obtingui accés sense fils a la xarxa:

- Sense una clau d'autenticació vàlida, el punt d'accés prohibeix el tràfic. Quan una estació sense fils entra a l'espai del punt d'accés, aquest envia un desafiament a l'estació.

- Quan l'estació rep el desafiament, respon amb la seva identitat. El punt d'accés envia

novament la identitat de l'estació a un servidor RADIUS que realitza els serveis d'autenticació.

- Posteriorment, el servidor RADIUS sol·licita els credencials de l'estació, especificant el tipus de credencials necessaris per confirmar la seva identitat.

- El servidor RADIUS valida els credencials de l'estació i transmet una clau d'autenticació al punt d'accés. La clau d'autenticació es xifra de manera que només el punt d'accés pugui interpretar-la.

- El punt d'accés utilitza la clau d'autenticació per transmetre de manera segura les claus correctes a l'estació, incloses una clau d'una difusió i un altre de sessió global per a les multi- difusions.

- Per mantenir la seguretat es pot demanar a l'estació que torni a autenticar-se periòdicament.

Evidentment, sembla un sistema massa complicat per instal·lar a la nostra xarxa local, així que no fa falta comentar-lo més.

## 4: RADIUS amb WEP de128-bits

El router permet una última opció (la 4ª) a la que combina el servidor RADIUS amb una clau de codificació WEP de 128 bits.

Personalment escolliria la segona opció, **WPA Pre-Shared Key.** És de les més segures i menys complicades de configurar.

# CONCLUSIONS

**Respecte al treball:**

Podem dir que l' ús més general del Bluetooth és l'intercanvi d'informació entre dispositius electrònics que es troben a curtes distàncies. Així podem per exemple, connectar el nostre PDA o càmera digital a l'ordinador sense fils al mig.

Per altra banda la Wi-Fi ofereix deu vegades més la velocitat d'intercanvi del Bluetooth. Aquesta tecnologia s'utilitza normalment per a les xarxes d'ordinadors sense fils, tant de xarxa local com d'Internet. Per exemple, en una empresa és necessari que diversos ordinadors es comuniquin entre ells. Aquí no ens val el Bluetooth perquè es requereix més velocitat de transmissió.

Llavors Wi-Fi o Bluetooth? Millor els dos. El fet de poder connectar-nos a una xarxa LAN a alta velocitat fa que la Wi-Fi s'utilitzi més per a la transmissió de paquets d'arxius, mentre que Bluetooth sigui més útil com a tecnologia de comunicació directa entre dispositius determinats, sense més complicacions. Els experts entenen que no existeix "incompatibilitat" entre les dues tecnologies i que contar amb les dues ens ajudarà a treure millor profit dels dispositius amb que contem.

**Personals:**

Ha sigut un treball molt interessant de fer. Tracta un tema que ens rodeja pràcticament sempre i del qual no ens adonem.

Gràcies a les immenses possibilitats que ofereix la Wi-Fi, pot arribar a ser el sistema de telecomunicació mòbil del futur, i quan parlem de telefonia mòbil, tots sabem que parlem d'actualitat i evolució contínua.

D'altra banda ha estat molt interessant investigar i trobar informació sobre tota la gent que fa

possible els processos de normalització i les associacions sense afany de lucre.

Saber que hi ha un munt de persones que creen organitzacions i que ofereixen accés a una xarxa interna de forma gratuïta... Que dedica la major part del seu temps lliure a muntar les antenes i a configurar els nodes, que gasten els diners de la seva butxaca, i tot per ajudar a l'altre gent, és un fet que crida l'atenció. Per què ho fan? Doncs perquè és un repte per ells, perquè ara existeix el codi lliure i coses que abans no eren possibles ara es poden aconseguir amb un seguit de coneixements i treball.

La part pràctica m'ha anat de perles. Vaig tenir el problema de muntar el meu nou router i gràcies a investigar en el seu moment he pogut incloure al treball tot el que vaig aprendre llavors.

Espero que aquest treball em serveixi en un futur. He après moltíssimes coses que estic segur que hem serviran de cara als pròxims anys. Tot plegat, ha valgut la pena.

# BIBLIOGRAFIA

ADSL-Ayuda. Seguridad Inalámbrica: Encriptación. Data de publicació del manual: 12 de desembre del 2005. Adreça d'accés: <http://www.adslayuda.com/wag54g-14.html>. [Última consulta 18 de gener del 2007]

Alonso, Chema. ¿Cómo proteger una red inalámbrica?. PC WORLD ONLINE. Publicat: 29 de novembre del 2006. Adreça d'accés a l'arxiu: <http://www.idg.es/pcworldtech/mostrar-Articulo.asp?id=297748118&seccion=seguridad>. [Última consulta 17 de gener del 2007]

Arnedo Moreno, Joan. Xarxes locals sense fils. UOC. Publicat: Febrer de 2002. Adreça d'accés: <http://www.uoc.edu/web/cat/art/uoc/arnedo0202/arnedo0202.html#3>. [Última consulta 17 de gener del 2007]

ComEsFa?org. Què és guifi-net?. Última actualització: 8 d'octubre del 2005. Adreça d'accés: <http://www.comesfa.org/ca/node/371>. [Última consulta 17 de gener del 2007]

Eduardo Aguirre, José. Redes Inalámbricas. Monografias. Publicat: 5 de febrer de 1999. Adreça d'accés: <http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml>. [Última consulta 18 de gener del 2007]

*El País* [en línia]. [Madrid: Premsa Española], c2007. San Francisco ofrecerá Internet gratis a todos sus ciudadanos. REUTERS. Publicat: 8 de gener del 2007. Arxiu dels números de l'últim mes a: <http://www.elpais.com/articulo/internet/San/Francisco/ofrecera/Inter-net/gratis/todos/ciudadanos/elpeputec/20070108elpepunet_1/Tes>. [Última consulta 16 de gener del 2007]

Morales, Marta. Crecen los puntos Wi-Fi de Internet en todo el mundo. Tendencias21. Publicat: 21 de novembre del 2006. Adreça d'accés: <http://www.tendencias21.net/Crecen-los-puntos-Wi-Fi-de-Internet-en-todo-el-mundo_a1243.html>.[Última consulta 16 de gener del 2007]