



epsc

**Escola Politècnica Superior
de Castelldefels**

UNIVERSITAT POLITÈCNICA DE CATALUNYA

TREBALL DE FI DE CARRERA

TÍTOL DEL TFC: Estudi i propostes de millora de la xarxa Guifi.net (I)

TITULACIÓ: Enginyeria Tècnica de Telecomunicació, especialitat Telemàtica

AUTOR: David Serra Pàmies

DIRECTOR: Roc Messeguer Pallarès

DATA: 1 de desembre de 2007

Títol: Estudi i propostes de millora de la xarxa Guifi.net (I)

Autor: David Serra Pàmies

Director: Roc Messeguer Pallarès

Data: 1 de desembre de 2007

Resum

La societat de la informació és cada cop més gran i s'encamina cada cop més a utilitzar dispositius mòbils, ja que la societat necessita la mobilitat. La relació entre qualitat, amplada de banda i preu de les ADSL encara no és gaire favorable, especialment la qualitat i la cobertura de les ADSL rurals.

Tot això ha provocat la creació de comunitats lliures d'intercanvi, a part d'Internet, utilitzant la tecnologia sense fils IEEE 802.11 que proporciona aquesta mobilitat a la societat de la informació. Les comunitats sense fils construïdes usant l'espectre obert permeten connectar la gent entre si des de qualsevol lloc. Una xarxa independent i global que estigui oberta a tothom pot ser molt valuosa, ja que les comunitats sense fils són una de les poques alternatives per a aconseguir una comunicació universal viable sense la intervenció d'intermediaris. Les comunitats de xarxes sense fils han experimentat un creixement i una extensió cada vegada més important gràcies a tots els beneficis que se'n poden obtenir.

Una d'aquestes comunitats Wi-Fi és Guifi.net. Aquesta comunitat disposa d'una xarxa sense fils que ha crescut de forma exponencial, la qual cosa ha provocat últimament una deterioració en el servei proporcionat per la comunitat. Aquesta deterioració ve donada pel fet que els medis sense fils tenen unes característiques diferents als altres medis, la qual cosa fa que els protocols utilitzats en la xarxa no siguin del tot eficients.

En aquest projecte s'han estudiat diferents protocols adaptats per a xarxes d'encaminament sense fils per a aconseguir minimitzar tots els problemes deguts al mitjà sense fils. Aquests protocols han estat provats en escenaris concrets per a veure el seu funcionament i extreure'n configuracions més eficients. L'entorn utilitzat en tot moment ha estat fidel a Guifi.net, des de la utilització del mateix hardware/software, fins a les topologies utilitzades.

Title: Study and proposals of improvement in the network Guifi.net (I)

Author: David Serra Pàmies

Director: Roc Messeguer Pallarès

Date: December, 1st, 2007

Overview

Today the informational society is growing up and it is going to use mobile devices more and more, because the society needs mobility. The relation between the quality, the bandwidth and the prices of ADSL is not good enough yet, especially what concerns the quality and the coverage in countryside.

These factors have caused the creation of free swapping communities aside Internet using the wireless technology IEEE 802.11, which provides us with this mobility in the informational society. Wireless communities constructed using the opened spectrum allow people to connect between themselves from anywhere. It may be very valuable an independent and global net opened to everybody. Wireless communities are one of the few alternatives to obtain a universal and viable communication, without intermediary. Wireless net communities have lived a growing and an expansion more and more important, thanks to all the benefits which can be obtained from.

One of those Wi-Fi communities is GUIFI.NET. It relies on a wireless net that has been growing recently in an exponential way, causing damage on its service. This damage results from the characteristics of the wireless environments, which are different from the other environments, so the protocols used in this net are not efficient enough.

In this project, several protocols adapted to routing wireless nets have been studied, in order to minimize the problems related with this type of connection. These protocols have been tested in determinates scenarios to have a look at its operation and to make more efficient configurations. The environment used during the whole work has been Guifi.net, from the using of the same hardware and software, to the typology used.

ÍNDEX

INTRODUCCIÓ	1
CAPÍTOL 1. GUIFI.NET: UNA XARXA OBERTA	3
1.1. Introducció	3
1.2. Les xarxes obertes sense fils.....	3
1.3. La xarxa Guifi.net.....	4
1.4. Serveis de Guifi.net	5
1.4.1. Serveis clàssics	5
1.4.2. Serveis multimèdia	5
1.5. Altres iniciatives a Catalunya.....	6
1.6. Altres iniciatives	6
CAPÍTOL 2. TECNOLOGIES UTILITZADES	7
2.1. Introducció	7
2.2. Hardware	7
2.2.1. Linksys WRT54GL.....	7
2.3. Software.....	8
2.3.1. OpenWRT	8
2.3.2. DD-WRT	9
2.4. Nivell d'enllaç.....	9
2.4.1. WLAN	9
2.5. Xarxes ad-hoc	10
2.6. Encaminament	10
2.6.1. Protocols proactius	10
2.6.2. Protocols reactius	11
2.7. Nivell de Xarxa	11
2.5.1. Túnel i OpenVPN.....	11
2.5.2. Protocol OLSR.....	11
2.5.3. B.A.T.M.A.N.....	12
CAPÍTOL 3. ESTUDI PRÀCTIC AMB OLSR.....	13
3.1. Introducció	13
3.1.1. Funcionalitats del nucli	13
3.1.2. Funcionalitats auxiliars	15
3.2. Primer escenari amb OLSR: encaminament.....	16

3.3. Segon escenari amb OLSR: mobilitat	18
3.4. Tercer escenari amb OLSR: seguretat	19
3.5. Quart escenari amb OLSR: rutes alternatives.....	20
3.6. Cinquè escenari: B.A.T.M.A.N.....	24
3.6.1. Millores introduïdes per B.A.T.M.A.N envers OLSR	25
CAPÍTOL 4. APLICACIÓ A GUIFI.NET	28
4.1. Introducció	28
4.2. Disseny de la xarxa d'accés	28
4.3. Disseny de la xarxa de distribució.....	33
4.4. Implicacions d'implantació.....	35
CAPÍTOL 5. CONCLUSIONS	36
5.1. Impacte medioambiental.....	36
5.2. Línies futures d'estudi	37
5.3. Avaluació personal de l'estudi.....	37
BIBLIOGRAFIA	39
ACRÒNIMS I SIGLES.....	40
ANNEX 1: PREPARACIÓ DELS WRT54GL	41
A1.1. Introducció	41
A1.2. Configuració OLSR	42
ANNEX 2: CONFIGURACIONS.....	44
A2.1. Introducció	44
A2.2. Escenari 1	44
A2.3. Escenari 2.....	46
A2.4. Escenari 3.....	48
A2.5. Escenari 5.....	48
ANNEX 3: THE WIRELESS COMMONS MANIFESTO.....	50
ANNEX 4: LLICÈNCIA COMUNS SENSEFILS.....	52

INTRODUCCIÓ

Les possibilitats que ofereix la tecnologia de comunicacions de dades sense fils han facilitat que arreu s'hagin construït múltiples comunitats, independents als nous models de negoci sobre xarxes, amb l'objectiu principal de connectar usuaris distants per poder, d'aquesta manera, posar en comú recursos i serveis. Com que aquests no estan sota el control d'una empresa amb ànim de lucre, els seu límits són el límit de les possibilitats tecnològiques, la imaginació i la capacitat de cada usuari.

Les comunitats Wi-Fi compleixen també una altra funció important: la de posar a l'abast de tothom les tecnologies tan aviat com algú estigui disposat a fer-ho, i no pas a conveniència d'estratègies comercials de grans empreses, que no sempre actuen segons les condicions de mercat i possibilitats tecnològiques, ja sigui per la seva posició dominant o en funció de la regulació existent.

Els beneficis que proporciona una xarxa amb aquest model són notables, ja que avui dia la tecnologia crea excedents en recursos que no sempre podem aprofitar de forma particular. Si es posen en comú, no es renuncia a ells i a canvi s'obté accés als que els altres estan a la vegada disposats a compartir. Guifi.net és una singular associació d'usuaris de xarxes sense fils a Catalunya. Aquesta és possiblement la que cobreix una extensió geogràfica més gran i, possiblement, la més activa, que esdevé tot un referent en el seu àmbit. Part dels usuaris mantenen una llista de correu on es debaten tots els temes de recerca i innovació que es duen a terme en aquesta associació.

En el primer capítol d'aquest document es realitza una introducció a les comunitats de xarxes obertes sense fils i en concret a la comunitat Guifi.net, que és on es desenvolupa aquest projecte. Es descriu la finalitat de la comunitat i les aplicacions i característiques de la xarxa. Per finalitzar aquest capítol, també es realitza una menció a altres comunitats catalanes i de fora de Catalunya.

En el segon capítol es realitza un recull de les tecnologies utilitzades a Guifi.net i les estudiades en aquest projecte. Es descriu el maquinari utilitzat en la xarxa, que també és l'utilitzat en l'estudi. També es descriu el software que s'utilitza en aquest maquinari amb les diferents distribucions de sistemes operatius que s'hi poden utilitzar. En la part de software també es desenvolupen les característiques d'una xarxa sense fils mòbil i els diferents protocols de comunicacions utilitzats. Dins d'aquest capítol també s'anuncien les propostes que es desenvoluparan posteriorment i que donaran com a resultat la resta de tasques d'aquest estudi.

El tercer capítol correspon a la segona part de desenvolupament d'aquest estudi. Dins d'aquest capítol es cobreixen els aspectes referents a l'aplicació del protocol OLSR. Aquest protocol es posarà en pràctica en diferents escenaris, on cadascun fa referència a les diferents problemàtiques que existeixen a Guifi.net. Cada escenari es muntarà per a estudiar i comprovar el funcionament de les característiques del protocol. Tenint en compte que per al

desenvolupament d'aquest estudi es disposa dels mateixos equips de hardware utilitzats a Guifi.net, es considera interessant el disseny, la realització i l'optimització de diferents escenaris amb el protocol. Mitjançant aquest protocol d'encaminament es pretén estudiar les possibles solucions a algunes problemàtiques, com l'escalabilitat de la xarxa, o introduir algunes millores com la mobilitat dels usuaris. En aquest capítol també es posa en pràctica el nou protocol sorgit fa relativament poc temps, derivat d'OLSR: B.A.T.M.A.N. Després de realitzar l'estudi pràctic d'ambdós protocols es realitza una comparativa entre ells.

En el cinquè capítol es pretén realitzar una proposta d'aplicació de les tecnologies estudiades en el cas particular de Guifi.net. En aquesta proposta s'apliquen tots els coneixements que han estat fruit de l'estudi teòric i pràctic dels anteriors capítols, per a aconseguir una xarxa amb menys problemes d'escalabilitat i amb més mobilitat. S'apliquen els protocols estudiats, optimitzant-los per a una xarxa de les característiques de Guifi.net, però deixant marge de llibertat per a una hipotètica implantació tot realitzant recomanacions sobre les variacions de valors, per tal que s'adapti correctament a cada cas particular. Aquesta proposta es basa en una arquitectura jeràrquica de la xarxa per a aconseguir l'escalabilitat necessària per a Guifi.net.

Finalment, en el sisè capítol es recullen les conclusions fruit de la realització de tot l'estudi i les propostes d'optimització. En aquest capítol també es realitzen les consideracions mediambientals del projecte i s'inclouen les línies futures que caldran desenvolupar.

CAPÍTOL 1. GUIFI.NET: UNA XARXA OBERTA

1.1. Introducció

Les possibilitats que ofereixen les tecnologies sense fils ha facilitat que arreu hagin sorgit múltiples comunitats per connectar amb el veïnat i, d'aquesta manera, poder posar en comú recursos i serveis que, en no estar sota el control d'una empresa amb ànim de lucre, només coneixen el límit de les possibilitats tecnològiques, la imaginació i la capacitat de cadascú.

L'objectiu principal de guifi.net és posar en comú la infraestructura i proporcionar els mecanismes d'organització per al seu funcionament i gestió. No és en cap cas una empresa, ni privada ni governamental, orientada a proporcionar un servei públic o de pagament, sinó simplement la coincidència en un interès comú del grup de persones que la forma. Enfocat d'aquesta manera, els beneficis que proporciona són notables: avui dia la tecnologia crea "excedents" que en recursos que no sempre podem aprofitar de forma particular, si els posem en comú no es renuncia a res i a canvi obtenim accés als que els altres estan a la vegada disposats a compartir amb nosaltres.

Les comunitats Wi-Fi compleixen també una altra funció important: la de posar a l'abast de tothom tecnologies tan aviat com algú estigui disposat a fer-ho i no pas només a conveniència d'estratègies comercials de grans empreses, que no sempre actuen segons les condicions de mercat i les possibilitats tecnològiques. Guifi.net també és un espai de recerca i desenvolupament per a la adaptació d'aquestes tecnologies a les finalitats que li són pròpies en una xarxa oberta.

1.2. Les xarxes obertes sense fils

La comunitat Guifi.net és una xarxa oberta. Cal distingir clarament el que és una xarxa oberta i lliure d'una de privativa. Cobrar o no cobrar per formar part d'una xarxa no és el que fa la diferència. De fet no hi té res a veure ni hi està relacionat.

Una xarxa lliure i oberta és aquella oberta a que hi participi tothom qui vulgui, en la modalitat que vulgui, on la xarxa en sí mateix no és propietat de ningú, i per definició és oberta a interconnexions amb altres xarxes, construint així una xarxa global. Si eventualment algú hi cobra alguna cosa, ho fa només en concepte d'un servei real, no pel sol fet de fer un "peatge" per accedir a una xarxa.

D'altra banda, una xarxa privativa és aquella en la que qui l'ha desplegat, la considera un actiu de la seva propietat i impedeix la interconnexió a d'altres xarxes encara que ho faci gratuïtament. Exemples d'aquests tipus de xarxes són les xarxes propietat de companyies i institucions o xarxes privades

d'usuaris. Altres xarxes privatives són les iniciatives com per exemple FON ja que no és una xarxa de propietat dels usuaris ni administrada per aquests.

El punt comú de totes les xarxes obertes és que s'adhereixen a un text, anomenat *The Commons Wireless Manifesto*. Aquest manifest és una declaració de motivacions per a crear les xarxes obertes i lliures. Les principals motivacions d'aquest text són els beneficis de la creació de xarxes obertes independents del control al que estan sotmeses les xarxes privatives. En aquest manifest també s'expliquen les barreres que existeixen per a la creació d'aquestes xarxes i reptes a assumir.

A banda del *The Commons Wireless Manifesto*, s'ha creat un altre text anomenat Comuns sense fils. El Aquest text és el resultat de traslladar els principis de codi lliure (GPL i similars) i creació lliure (Creative Commons i similars) a l'activitat de fer xarxa oberta. Aquesta llicència s'ha redactat per crear un marc específic per a crear una forma de fer xarxa oberta i un marc on els diferents agents que intervinguin en aquest tipus de xarxa s'hi puguin acollir i els serveixi de referent de com relacionar-se.

L'objectiu d'aquesta llicència és recuperar d'alguna manera el que havien estat els principis de Internet: Fer una xarxa de caràcter universal, però en aquest cas prescindint de les regulacions que s'han establert a través dels proveïdors d'accés. D'aquesta manera qualsevol persona a títol individual o col·lectiu disposa d'un marc on estableix quins son els principis i funcionament de la xarxa.

En relació a la legalitat d'aquestes xarxes, s'ha de notar que utilitzen l'espectre radioelèctric que no requereix llicència ja que transmeten a 2,4GHz o bé a 5GHz i és ús particular i limitat en abast. Donat que s'emmarca dins de l'autoprestació de serveis de comunicació tampoc requereix de llicència d'operador ni de comunicació a la CMT.

1.3. La xarxa Guifi.net

Actualment la xarxa Guifi.net disposa de més de 3.000 nodes operatius. Aquesta xarxa disposa d'una topologia en forma de malla i està formada per dos grans parts: la part troncal, que s'encarrega d'intercomunicar les diferents zones, i els "punts guifi.net" o "nodes", des d'on es proporciona cobertura als clients.

La part troncal són enllaços típicament configurats com a enllaços entre dos punts i gestionats de forma comuna entre tots. Aquests enllaços, com que són els encarregats de distribuir tot el tràfic a la xarxa, són enllaços més estables i estan gestionats amb especial atenció orientats a la màxima disponibilitat, amplada de banda i seguretat.

Els "punts calents", o "punts guifi.net", ja són els nodes que cadascú munta i gestiona lliurement per qui es se'n vulgui fer responsable. Per a aquests nodes s'utilitza la tecnologia que cadascú tingui disponible al seu abast i vulgui amb la

única restricció de no perjudicar el bon funcionament de la xarxa troncal. Accepta o no connexions lliurement de qualsevol client, en funció dels criteris de qui els administren.

Les adreces s'assignen amb compatibilitat a l'adreçament de freenetworks.org. Aquesta iniciativa pretén assignar adreçament privat d'una forma jeràrquica i topològicament vàlida a tots els clients que s'hi vulguin adherir. La única condició és permetre el lliure trànsit, com si es tractés d'una rèplica de l'Internet actual. L'aplicació anirà assignant de forma automàtica les adreces als usuaris i als enllaços d'acord amb els rangs que assignin els administradors de cada zona.

1.4. Serveis de Guifi.net

En la xarxa Guifi.net es comparteixen una sèrie de serveis entre tots els seus usuaris. A diferència dels serveis comercials, aquests estan administrats pels mateixos usuaris que els comparteixen i, per tant, la seva disponibilitat o capacitat està limitada als recursos que aquest usuari pugui o vulgui aportar. Tot i això, la cartera de serveis que aporta Guifi.net és més innovadora i avançada que qualsevol opció comercial per al gran públic.

1.4.1. Serveis clàssics

Tots els anomenats serveis clàssics de la pila TCP/IP estan implementats en diferents servidors, tots en l'entorn Linux. El parc de servidors distribuït aporta a la xarxa un nom de domini registrat (guifi.net) i una capacitat d'emmagatzematge de fitxers (FTP) per a tothom. A tots els usuaris que ho desitgin, Guifi.net els proporciona un compte de correu electrònic del domini, accessible mitjançant diferents mecanismes (POP/IMAP, SSL,...) i proporciona allotjament de pàgines d'usuari. En aquest punt, existeix una àmplia diversitat quant a programari ja operatiu als diversos servidors, així com disponibilitat de pàgines dinàmiques i accés a bases de dades. També existeix un servidor de missatgeria en línia (IRC) que realitza la funció de passarel·la amb la resta de canals existents a Internet. Per últim, alguns usuaris han habilitat portes a Internet i les cedeixen a qui les vulgui utilitzar. La llista està permanentment monitorada i publicada.

1.4.2. Serveis multimèdia

En el node bandoler.guifi.net es troba un servei de veu sobre IP (VoIP). El node disposa d'un servidor Asterisk. El servei és accessible des de Guifi.net, i també via NAT i Internet. Compta amb bústies de veu, amb avís de missatges via SMS i correu electrònic. Tothom hi pot crear extensions. En l'actualitat existeixen serveis de pagament semblants, com és el cas de l'iPhone d'Al-Pi Telecomunicacions, però els grans operadors actualment no ofereixen cap tipus de suport ni servei semblant.

1.5. Altres iniciatives a Catalunya

La iniciativa Guifi.net no és única ni pionera a Catalunya, ja que actualment n'existeixen fins a un centenar, que cobreixen gran part del territori. Tots aquests grups de treball convergeixen sota uns objectius i metodologies semblants. Des de fa temps totes aquestes organitzacions s'agrupen per realitzar trobades i posar en comú algunes experiències i coneixements. Algunes d'aquestes comunitats són per exemple Mataró SenseFils i Olot wireless.

1.6. Altres iniciatives

Per completar l'estat de l'art de les xarxes lliures sense fils s'ha de comentar que aquest moviment no és únic ni està subjecte a classes o distincions arreu del planeta. Dins l'estat espanyol també existeixen moltes comunitats obertes. És considera important anomenar la comunitat que s'ha muntat a Guadalajara, sota el nom de Guadawireless². Aquesta iniciativa segueix el mateix model i les mateixes eines tecnològiques que Guifi.net. La seva xarxa compta amb els mateixos serveis, als que cal afegir la missatgeria instantània i els jocs en xarxa. Com a característica semblant, Guadawireless també compta amb un sistema per georeferenciar els nodes i mostrar-ho de forma dinàmica amb el portal propi.

Possiblement el moviment més semblant a Guifi.net, amb el mateix model característic però amb una extensió molt més gran, és AthensWireless³. Aquesta iniciativa compta amb més de tres mil nodes dins de la seva xarxa i els mateixos serveis. També són molt conegudes les comunitats de Seattle, Nova York, París i Berlín. Paral·lelament a l'aparició de tantes comunitats sense fils i tant variades, han sorgit altres comunitats virtuals, també anomenades metacomunitats. Una de les funcions socials que absorbeixen són la comunicació i la integració entre les diferents comunitats existents. Les més conegudes són Freenetworks, Freifunk i Redlibre, la primera ja comentada en aquest capítol, ja que Guifi.net segueix el seu pla d'adreçament.

Totes les comunitats nombrades fins el moment tenen en comú que són lliures i estan impulsades pels propis usuaris. Tanmateix, també existeixen altres moviments promoguts amb ajuts públics o privats: qualsevol ajuntament que instal·li una xarxa sense fils al municipi i l'ofereixi a baix cost als seus usuaris n'és un exemple.

CAPÍTOL 2. TECNOLOGIES UTILITZADES

2.1. Introducció

Un cop explicat l'entorn social en què es realitza aquest estudi cal veure en quin entorn tecnològic es desenvolupa. Aquest punt és necessari amb la finalitat de conèixer de quines eines (hardware i software) es disposa per realitzar aquest estudi i exposar en quines tecnologies es vol centrar. Aquest capítol també pretén presentar aquestes tecnologies i anomenar els coneixements mínims necessaris per continuar la lectura del següent capítol. Per complementar la informació, el lector es pot adreçar a l'annex primer, titulat "Preparació dels WRT54GL".

Per últim, es considera important la redacció d'aquest punt per tal d'obtenir una llista de propostes realitzables pel que fa a l'entorn tecnològic i a la seva disponibilitat.

2.2. Hardware

La xarxa Guifi.net es basa en una xarxa amb dos tipus d'equips. Per una banda es troben els equips de la xarxa troncal, que són un equipament comú i, per tant, gestionat per tota la comunitat. Aquests equips estan orientats a utilitzar-los com a equips d'alta disponibilitat i per a enllaços de llarga distància. Per l'altra banda es troben els equips particulars que cadascú munta i configura lliurement. Cal dir que la majoria d'equips són del fabricant Linksys.

Per a la realització d'aquest estudi es disposa de tres punts d'accés sense fils del mateix fabricant, Linksys, el model dels quals és el WRT54GL.

2.2.1. Linksys WRT54GL

WRT54 és el nom d'una saga molt popular de routers fabricats per Linksys filial corporativa de Cisco Systems. Els routers d'aquesta sèrie permeten interconnectar diversos dispositius de xarxa mitjançant els enllaços Ethernet 802.3 i 802.11g sense fils.

El primer model de la sèrie va ser el WRT54G. Les 5 primeres versions d'aquest model utilitzaven un firmware basat en Linux. A partir d'aquesta versió, es van disminuir les memòries Ram i Flash i es va començar a utilitzar el sistema operatiu VxWorks.

El model WRT54GS incorpora la tecnologia SpeedBooster i inclou més memòria (tant Ram com Flash) que el model WRT54G. Aquest model, igual que el WRT54G, inclou un sistema operatiu Linux fins a la versió 5 i a partir d'aquesta comença a utilitzar el VxWorks.

Es disposa del model WRT54GL per a la realització d'aquest estudi. Aquest model va aparèixer després de la versió 5 del model WRT54G i torna a portar un sistema operatiu basat en Linux tot i que, a diferència del WRT54GS, no incorpora la tecnologia SpeedBooster. Quant a la memòria que incorpora, s'ha de dir que porta la mateixa que el model WRT54GS, és a dir, més que els primers models WRT54G.

Aquest equip incorpora 3 interfícies de xarxa, les dues primeres són Ethernet 802.3 (per als enllaços WAN i LAN) i la tercera és una interfície ràdio Ethernet 802.11 (WLAN). La potència de transmissió màxima és de 18dBm. L'equip és compatible amb els estàndards "b", "g" i "n" de la norma 802.11.

2.3. Software

Existeixen diversos projectes de desenvolupament de firmware compatibles amb el hardware que es disposa. Com a projectes més importants destaquen els següents: HyperWRT Thibor, Sveasoft, Tomato, DD-WRT i OpenWRT. Dels mencionats anteriorment només es consideren els dos últims, ja que són els projectes que disposen de la màxima disponibilitat d'aplicacions i llibreries software i que permeten més llibertat d'operació. Tots dos projectes estan basats en Linux amb llicència GPL.

A part d'aquests dos projectes també es considera el Freifunk, una distribució basada en el OpenWRT. Aquest, a més de la base del OpenWRT, ja inclou preinstal·lats els paquets per al suport de xarxes mallades amb protocol OLSR i un interfície web d'administració capaç de modificar còmodament els paràmetres d'aquest protocol.

2.3.1. OpenWRT

La distribució OpenWRT està especialment pensada per a sistemes Wi-Fi embotrats i distribuïda sota llicència GPL. En comptes d'introduir el màxim de funcionalitats possibles en la distribució, només es proporciona un firmware amb el mínim de capacitats. Per als usuaris amb coneixements avançats de Linux hi ha suport per afegir una varietat molt àmplia de paquets i programari, afegint les funcionalitats que es desitgen de forma modular.

Com que OpenWRT es tracta d'una distribució oberta, els usuaris desenvolupen o adapten altres programaris existents. Així doncs, OpenWRT és la distribució amb el màxim de funcionalitats disponibles: dimonis d'encaminament, VLANs, VoIP, encriptació, seguretat i una extensa llista.

Per últim cal comentar que aquesta distribució també és compatible amb equipament de D-Link, Asus, Dell, Buffalo, Motorola, Toshiba i US-Robotics, entre d'altres.

2.3.2. DD-WRT

DD-WRT és la segona distribució més versàtil de les compatibles amb el Linksys WRT54GL. Es tracta d'un programari totalment lliure i distribuït sota llicència GPL.

L'última versió de DD-WRT, anomenada v23, és un projecte totalment nou respecte de la primera iniciativa. Les funcionalitats són tant o més àmplies que en el cas de l'OpenWRT. És d'especial interès anomenar-ne algunes de diferencials, com el suport inicial per IPv6, QoS i una interfície Web amigable.

Per últim, i igual que en la distribució anterior, cal comentar que DD-WRT també és compatible amb equipaments d'Asus, Siemens, Motorola, Buffalo i Allnet.

2.4. Nivell d'enllaç

La capa d'enllaç de dades correspon al nivell 2 del model OSI i s'encarrega de respondre a peticions de servei de la capa de xarxa i d'entregar les peticions a la capa física.

La capa d'enllaç de dades és la capa encarregada de transferir dades entre nodes de xarxa adjacents en una WAN o entre nodes del mateix segment de LAN. La capa d'enllaç de dades proporciona les funcions i els procediments per a la transmissió de dades entre entitats de xarxa i pot detectar i, fins i tot, corregir errors que poden ocórrer a la capa física. Alguns exemples de protocols d'enllaç de dades són Ethernet per a xarxes d'àrea local i PPP, HDLC i ADCCP per a connexions punt a punt.

L'enllaç de dades proporciona una transferència de dades al llarg de l'enllaç físic. Aquesta transferència pot ser fiable i pot no ser-ho. Molts protocols d'enllaç de dades no disposen de reconeixement de recepció i acceptació de trames amb èxit i, fins i tot, alguns protocols ni tant sols disposen de checksum per tal de comprovar errors en la transmissió. En aquests casos, certs protocols d'un nivell més alt han d'encarregar-se de proporcionar un control de flux, una comprovació d'errors i un reconeixement i retransmissió.

2.4.1. WLAN

La tecnologia WLAN està regida per l'estàndard 802.11, especificat per l'Institute of Electrical and Electronics Engineers (IEEE), el mateix organisme encarregat d'especificar la resta de tecnologies de xarxa (com l'Ethernet). Mitjançant aquest procés, es garanteix inicialment la interoperabilitat entre diferents fabricants i un funcionament dins les capes del model de comunicacions igual que qualsevol altra tecnologia de LAN. Per tant, la seva interacció amb protocols de comunicació, com TCP/IP, és totalment transparent. Des del punt de vista del sistema operatiu, emprar un adaptador de WLAN és igual que fer-ne servir un de LAN tradicional.

Aquest projecte no estudia aspectes ràdio ni del canal, però sí que es considera important aquesta breu menció, ja que pel fet d'utilitzar una tecnologia sense fils i un medi hostil, els enllaços poden tenir una disponibilitat variable. Aquesta condició pot afectar a les capes superiors (nivell de xarxa) d'una forma diferent de per la qual han estat ideats. A més, es considera interessant aquesta menció, donat que les tecnologies basades en 802.11 utilitzen una banda lliure de l'espectre i, per tant, on tothom pot transmetre sense llicència.

2.5. Xarxes ad-hoc

Una xarxa ad-hoc és un conjunt de nodes o hosts que es comuniquen entre si mitjançant enllaços sense fils sense la necessitat d'una infraestructura de xarxa fixa. Cada node actua com un router encaminant els paquets cap als terminals que es corresponen a les rutes cap al node destí sense la necessitat de que existeixi un enllaç directe entre la font i el destí del paquet.

Aquesta tipologia de xarxa és autònoma entre terminals que es poden moure lliurement. Els nodes d'una xarxa ad-hoc utilitzen taules d'encaminament per a organitzar les rutes cap a un destí i poder trobar sempre la millor ruta cap al destí del paquet. Aquestes taules d'encaminament s'han d'anar actualitzant amb una freqüència bastant elevada en comparació amb una xarxa cablejada, ja que en aquest tipus de xarxa, al existir-hi nodes mòbils, aquests poden canviar de posició. Quan la topologia canvia pel canvi de posició d'un node, la xarxa torna a calcular les rutes cap al node i torna a crear les taules d'encaminament més adequades per a poder arribar a qualsevol node de la xarxa.

2.6. Encaminament

Els protocols d'encaminament estan classificats bàsicament en dos grups: els proactius i els reactius segons la manera que utilitzen per a calcular les taules d'encaminament de la xarxa.

2.6.1. Protocols proactius

En els protocols proactius, s'envia informació d'encaminament periòdicament, tot i que no s'estigui enviant informació, per a que qualsevol node sigui capaç de comunicar-se amb qualsevol altre de la xarxa. Aquesta característica proporciona una resposta molt ràpida a sol·licituds de ruta i ofereix un bon comportament en situacions on la taxa de mobilitat és alta. Tanmateix la sobrecàrrega que s'introdueix a la xarxa amb la informació de control és alta en comparació amb els protocols reactius.

2.6.2. Protocols reactius

En els protocols reactius els nodes únicament disposen de rutes d'encaminament a les taules quan un node origen ha de realitzar una comunicació amb un altre node de la xarxa. En aquests protocols, al iniciar una comunicació i no tindre la ruta per a arribar a un node destí, s'envia un missatge de descobriment de ruta. Quan rep la resposta afegeix aquesta ruta a la seva taula d'encaminament i és llavors quan pot realitzar una comunicació amb aquest node destí. El principal inconvenient és la latència a l'hora de descobrir una nova ruta al principi de les comunicacions. Tanmateix aquests protocols al no estar calculant constantment taules d'encaminament aprofiten millor els recursos de xarxa i energètics dels terminals.

2.7. Nivell de Xarxa

La capa de xarxa, també anomenada capa d'Internet, es troba entre la capa d'enllaç de dades i la capa de transport, i s'encarrega de l'encaminament dels missatges, és a dir, determina la ruta des de l'origen fins el destí. La capa de xarxa també gestiona els problemes de trànsit, el control de la congestió de paquets de dades i la reordenació de paquets un cop arribats a la màquina de destí. També és la capa encarregada de traduir adreces lògiques i noms en adreces físiques.

2.5.1. Túnel i OpenVPN

La tècnica de tunneling consisteix en encapsular un protocol de xarxa per sobre d'un altre creant un túnel a dintre d'una xarxa de comunicacions i, d'aquesta manera, la comunicació entre ambdós nodes extrems és completament transparent per al protocol de xarxa de la xarxa de comunicacions l'alberga.

OpenVPN és un aplicatiu de xarxa privada virtual de codi obert que permet, entre altre moltes coses, crear túnels encriptats entre dos nodes. OpenVPN va ser creat per James Yonan la tardor de 2001 i publicat sota llicència GNU GPL.

2.5.2. Protocol OLSR

El protocol OLSR va ser creat per Thomas Clausen i Philippe Jacquet en el projecte Hipercom INRIA. Es tracta d'un protocol d'encaminament proactiu per a connectar xarxes sense fils ad-hoc mallades. L'OLSR és una optimització del clàssic algoritme d'estat de l'enllaç adaptat a les necessitats de les xarxes mòbils.

El concepte clau del protocol és el del Multipoint relays (MPR). Els MPR són els nodes seleccionats per a distribuir la informació de control de la tipologia de la xarxa mitjançant l'ús de missatges TC (Topology Control). Amb la informació continguda en aquests missatges TC, tots els nodes sense fils poden crear i

mantenir actualitzades les seves taules d'encaminament. La informació sobre l'estat de l'enllaç s'extrau de la transmissió de missatges Hello que permeten a cada node descobrir el conjunt de nodes veïns a un salt.

2.5.3. B.A.T.M.A.N.

OLSR-NG és un projecte open source que té com a objectiu la creació d'un nou RFC que millori l'OLSR actual. L'algoritme que a hores d'ara és el candidat amb més possibilitats d'esdevenir el nou RFC és el del projecte B.A.T.M.A.N..

B.A.T.M.A.N. (Better Approach To Mobile Ad-hoc Networking) és un projecte per a la creació d'un nou protocol d'encaminament proactiu per a connectar xarxes sense fils ad-hoc mallades.

CAPÍTOL 3. ESTUDI PRÀCTIC AMB OLSR

3.1. Introducció

L'OLSR és un protocol desenvolupat per a xarxes mòbils ad-hoc que opera en mode proactiu. Cada node selecciona un grup de nodes veïns com a "multipoint relay" (MPR), que són els responsables de la retransmissió del tràfic de control. Aquests nodes també tenen la responsabilitat de declarar l'estat de l'enllaç als nodes que l'han seleccionat com a MPR.

L'OLSR és un protocol modular. Té un nucli amb les funcionalitats que sempre són requerides per a funcionar i un conjunt de funcionalitats extres.

3.1.1 Funcionalitats del nucli

Les funcionalitats del nucli especifiquen el comportament d'un node amb OLSR. Això incorpora l'especificació universal dels missatges del protocol i la seva transmissió per la xarxa, així com la percepció dels enllaços, la difusió de la topologia de la xarxa i el càlcul de rutes.

- Percepció del veí
Per a saber l'estat de l'enllaç s'utilitzen els missatges "HELLO". El propòsit d'aquesta funcionalitat és que cada node tingui associat un estat de l'enllaç amb cadascun dels seus veïns. L'estat d'un enllaç pot ser simètric (l'enllaç verificat és bidireccional) y asimètric que indica que els missatges "HELLO" s'han rebut però que no podem assegurar que aquest node escolti les respostes.
- Detecció del veí
Donada una xarxa de nodes amb una sola interfície, un node ha de deduir els veïns que té mitjançant la informació intercanviada durant la percepció de l'enllaç. Cada node té guardats el grups de veïns. Cada veí ha de tenir associat un estat de l'enllaç. Quan es detecta l'aparició d'un nou enllaç s'ha de crear una entrada amb el veí que té un enllaç associat i en aquesta entrada també s'ha de guardar l'estat de l'enllaç. S'ha de tenir en compte que cada cop que varia l'estat de l'enllaç s'ha de comprovar a la taula que el canvi s'ha dut a terme. Si no es rep informació de l'enllaç durant un temps establert s'ha d'esborrar l'enllaç en qüestió i el veí associat.
- Selecció d'MPR i senyalització MPR
La selecció dels MPR serveix per a triar els nodes veïns que transmetran els missatges de control. La senyalització ve donada mitjançant missatges "HELLO". Cada node tria un o més MPR de manera que s'assegura que a través dels MPR seleccionats, cada node arriba a tots els veïns a dos salts.

En la figura 3.1 es pot observar com el node central (A) tria el mínim nombre de nodes a un salt (nodes C, G, E, I) capaços d'arribar a tots els nodes a dos salts de distància.

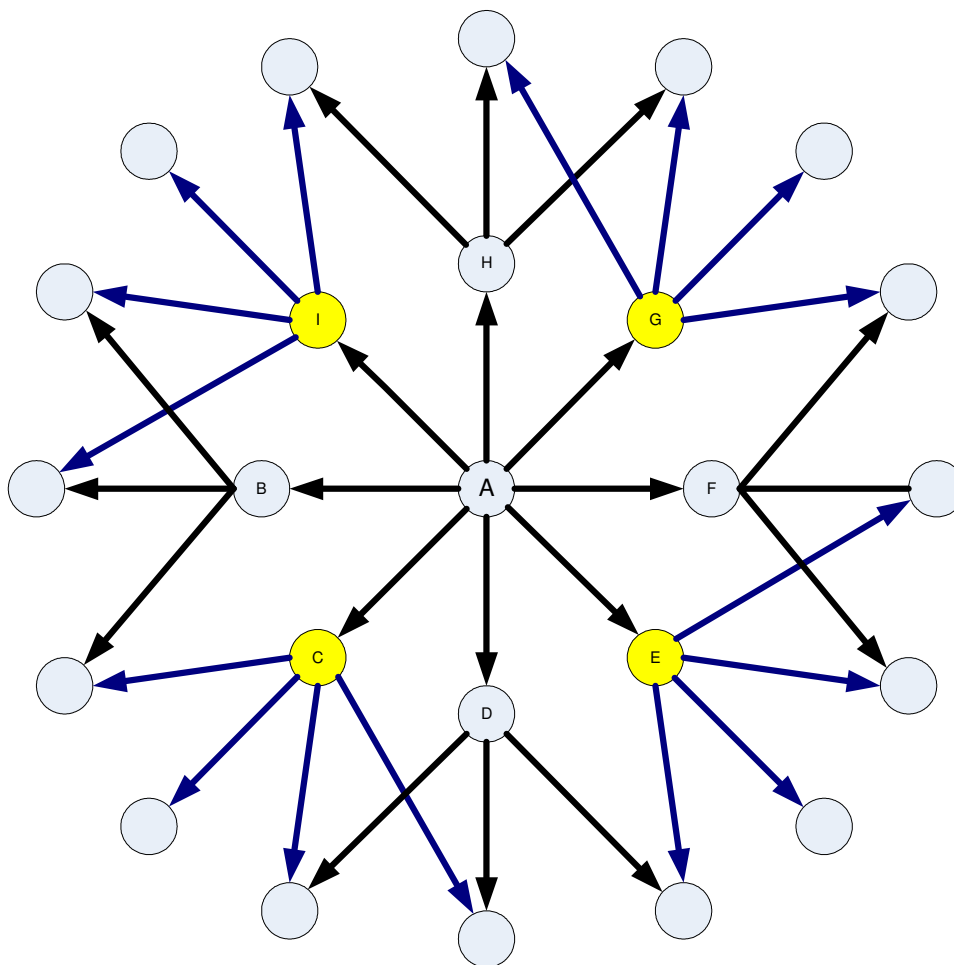


Fig. 3.1 Selecció dels nodes MPR

- Difusió dels missatges de control de topologia
Aquests missatges es difonen amb l'objectiu de donar a cada node de la xarxa la informació necessària per a permetre el càlcul de rutes. Són els missatges anomenats TC (Topology Control). Aquests missatges, que retransmeten un node cap als seus veïns seleccionats com a MPR, tenen la informació de tots els seus enllaços per a que els altres nodes sàpiguen els veïns als que pot arribar.
- Càlcul de rutes
Donada la informació de l'estat de l'enllaç que s'adquireix mitjançant l'intercanvi de missatges periòdics, cada node manté una taula d'encaminament que permet encaminar els paquets destinats a altres nodes. Aquesta taula està basada en la informació continguda en les bases d'informació d'enllaç i de la topologia. Aquesta taula s'actualitza quan es detecta algun canvi en alguns dels següents camps: l'enllaç, el

veí, el veí a dos salts o la topologia.

3.1.2. Funcionalitats auxiliars

Existeixen situacions on són necessàries unes funcionalitats auxiliars. Com per exemple un node amb múltiples interfícies on alguna de les quals participa en un altre domini d'encaminament.

- **Interfícies no-OLSR**
Hi ha nodes que poden tenir interfícies que no són OLSR. Aquestes interfícies poden ser de connexions punt a punt o poden connectar amb altres xarxes. Per a poder tenir connectivitat entre les interfícies OLSR i aquestes altres, el router ha de ser capaç d'introduir informació externa d'encaminament a la xarxa. Per això les interfícies no-OLSR creen un missatge Host and Network Association (HNA) que conté informació suficient per a poder crear noves rutes amb aquesta informació.
- **Notificació de la capa d'enllaç**
OLSR no treballa amb informació de la capa d'enllaç. Tanmateix, si la informació d'aquesta capa està disponible, aquesta informació pot ser utilitzada a més de la informació dels missatges "HELLO" per a mantenir la informació dels veïns i els MPR.
- **Percepció del veí de nivell avançat**
La percepció del veí de nivell avançat és un paquet de mesures destinades a fer que el mecanisme de percepció de veí resulti més robust. Entre aquestes mesures es troben la utilització de més atributs associats a un enllaç i mecanismes avançats per a detectar correctament l'estat dels enllaços.
- **Informació redundat de topologia**
Per a poder proveir redundància a la informació de la topologia, la informació d'anunci que emet el node ha de tenir informació d'enllaç cap a nodes veïns que no necessàriament tinguin a aquest node com MPR. El missatge d'anunci publica informació de tots els enllaços dels nodes veïns. Hi ha tres possibles nivells de redundància:
 - Redundància nul·la: només s'emet informació del grup que ha elegit el node com a MPR.
 - Redundància mitjana: s'emet informació del grup que ha elegit el node com a MPR i també s'emet informació sobre els nodes que aquest ha triat com a MPR.
 - Redundància alta: s'emet informació de tots els enllaços cap als veïns.
- **MPR redundat**
Aquesta funcionalitat especifica l'habilitat del node de seleccionar MPR

redundants. Tot i que la redundància crea molt més tràfic i el mecanisme de MPR perd eficiència, s'obté un gran guany en assegurar l'arribada dels paquets als seus destins. Aquesta funcionalitat és útil per a situacions on la xarxa té molta mobilitat i per a mantenir una bona cobertura amb els MPR.

3.2. Primer escenari amb OLSR: encaminament

Una xarxa en mode ad-hoc permet que un node només accedeixi als nodes amb els quals té un enllaç directe. OLSR, en canvi, proporciona un sistema de routing que permet que els nodes accedeixin a altres nodes amb els quals no tenen un enllaç directe.

Aquest primer escenari pretén estudiar el funcionament bàsic d'una xarxa sense fils amb el protocol OLSR. La xarxa està formada per tres encaminadors sense fils amb el protocol OLSR. En un d'ells penja un ordinador personal i en un altre es té connexió a Internet. Tant l'ordinador com l'accés a Internet es realitza mitjançant un port del switch Ethernet de cadascun dels routers.

Una altra característica de la xarxa és que entre el router que està connectat a Internet i el que ho està l'ordinador personal no hi ha cobertura, és a dir, no hi ha connexió física sense fils entre els routers A i C, ja que es troben a una distància superior a la que els permetria d'estar connectats directament. Al contrari que passa amb la connexió entre A i C, els enllaços A - B i B - C sí que es troben a una distància que permetrà que s'estableixi un enllaç.

L'objectiu d'aquest escenari és aconseguir configurar els 3 routers per a que, un cop posats en marxa, tots els dispositius de la xarxa puguin accedir a Internet des de l'ordinador personal. Això voldrà dir que s'hauran creat els enllaços A - B i B - C i les rutes adequades que permetran que l'accés a Internet funcioni correctament des de l'ordinador personal.

Per a que els nodes coneguin quin és el router que té accés a Internet, s'ha d'utilitzar el camp HNA4. Aquest camp permet a un node informar als altres nodes que utilitzen OLSR sobre quina és la porta d'accés a una xarxa concreta. Per tant, per a que el node C informi els altres nodes de quina és la porta de la xarxa cap a Internet, s'ha introduït el valor "0.0.0.0/24" al camp HNA4 del node C.

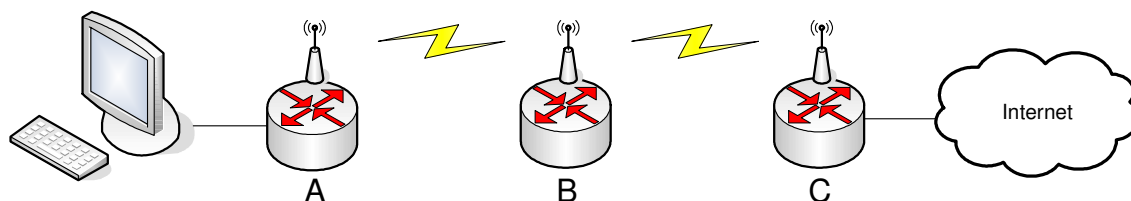


Fig. 3.1 Primer escenari amb OLSR

Aquest escenari permet testejar el sistema d'encaminament que proporciona OLSR. Mirant les taules de rutes del protocol es poden veure els enllaços creats, els nodes veïns de cada router i el rol adoptat per cada router.

A continuació es pot veure les taules de veïns i de rutes del node A obtingut durant l'experiència pràctica:

Node A: 192.168.1.1

Node B: 192.168.1.2

Node C: 192.168.1.3

Taula de veïns:

IP	Hysteresis	LinkQuality	lost	total	NLQ	ETX
192.168.1.2	0.00	0.44	56	100	0.40	5.68

Taula de rutes:

```
192.168.1.2      dev eth1 scope link metric 1
192.168.1.3      via 192.168.1.2 dev eth1 metric 2
```

Taula HNA:

Network	Netmask	Gateway
0.0.0.0	0.0.0.0	192.168.1.3
192.168.2.0	255.255.255.0	192.168.1.1

Realitzant un ping a un lloc web d'Internet podem comprovar que el protocol funciona correctament encaminant els paquets entre tots els nodes intermitjos:

```
C:\Documents and Settings\Administrator>ping www.google.es
```

```
Haciendo ping a google.navigation.opendns.com [208.69.34.230] con 32 bytes de datos:
```

```
Respuesta desde 208.69.34.230: bytes=32 tiempo=79ms TTL=253
Respuesta desde 208.69.34.230: bytes=32 tiempo=79ms TTL=253
Respuesta desde 208.69.34.230: bytes=32 tiempo=80ms TTL=253
Respuesta desde 208.69.34.230: bytes=32 tiempo=79ms TTL=253
```

```
Estadísticas de ping para 208.69.34.230:
```

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 79ms, Máximo = 80ms, Media = 79ms

En l'annex 2 es pot trobar un petit anàlisi de càrrega de CPU del node B d'aquest escenari. En aquest anàlisi es pot observar que la càrrega de CPU és molt baixa atès que el nombre de nodes de l'escenari és molt petit.

3.3. Segon escenari amb OLSR: mobilitat

El segon escenari pretén estudiar la possibilitat d'afegir mobilitat a la xarxa. Tal com està muntada ara la xarxa GUIFI.NET no permet mobilitat. En cas que un node es mogui dins les zones de cobertura de diferents nodes, l'usuari ha de canviar la connexió i la configuració per tal de connectar-se a un altre router.

OLSR permet que tot aquest procés sigui completament transparent per a l'usuari. Un node actualitza els seus veïns de forma constant. En el cas que es trobi un node veí, aquest passa a ser utilitzat dins la xarxa. També al contrari, si un node deixa de tenir cobertura sobre un altre, l'enllaç entre ells desapareix i es deixa d'utilitzar. Tot aquest procés permet a un usuari mòbil el fet que només li és precís tenir almenys cobertura d'un altre node per a poder estar enllaçat a la xarxa. El sistema funciona de manera que l'usuari és inconscient de quins són els routers veïns de què disposa cobertura, ni quins són els enllaços que s'estan utilitzant, donat que ell tan sols es connecta a la xarxa amb l'ESSID com a nom i sense saber quins nodes componen la xarxa. Per tant, tot l'escenari serà vist com un sol punt d'accés que dóna servei a una àrea més extensa i amb molta més capacitat de la que tindria un de sol.

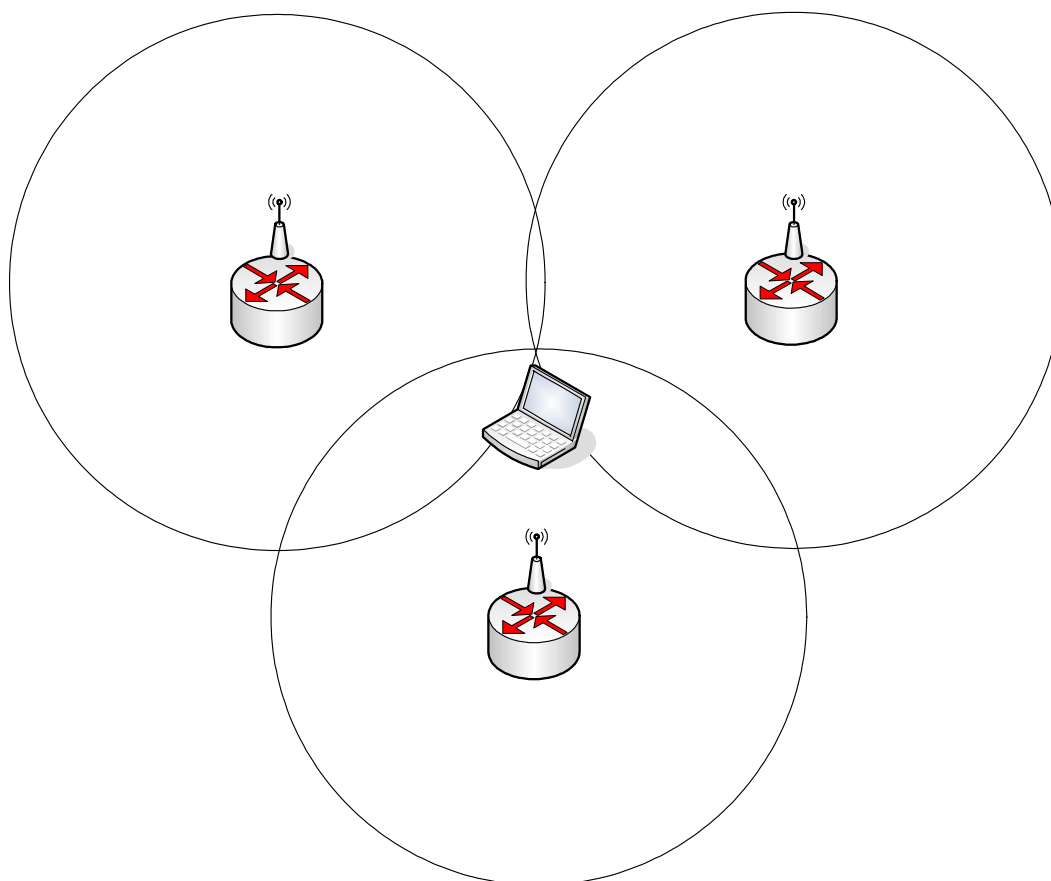


Fig. 3.2 Segon escenari amb OLSR

Per a testejar la funcionalitat de la mobilitat que permet OLSR, mitjançant un ordinador portàtil, ens desplaçarem per les diferents zones de cobertures que corresponen a cada router.

3.4. Tercer escenari amb OLSR: seguretat

En una xarxa ad-hoc existeixen problemes greus de seguretat que s'han de considerar. Alguns d'aquests problemes són relatius a la pròpia naturalesa dels enllaços sense fils i d'altres ja existeixen en les xarxes cablejades.

Com que OLSR és un protocol proactiu, periòdicament difon informació sobre la topologia de la xarxa. En cas que s'estigui utilitzant una xarxa wireless sense protecció, aquesta informació és revelada a tothom que es trobi escoltant els missatges de control del protocol.

En els casos en què la confidencialitat de la topologia de la xarxa és important, com és el cas de l'intercanvi de missatges OLSR de control de tràfic, pot ser útil utilitzar tècniques d'encriptació que permetin que els missatges només puguin ser llegits per a qui estigui autoritzat a fer-ho.

En OLSR, cada node injecta informació sobre la tipologia de la xarxa transmetent missatges del tipus HELLO, i alguns nodes, missatges TC. Si algun node, per qualsevol raó, malintencionada o per un mal funcionament, injecta missatges erronis, la integritat de la xarxa es pot veure compromesa. Alguns exemples de situacions que poden ocórrer per una manca de seguretat són:

- Un node que genera missatges TC publicant enllaços cap a nodes del que no n'és veí.
- Un node que genera missatges TC fent-se passar per un altre node.
- Un node que genera missatges HELLO publicant nodes dels que no n'és veí.
- Un node que genera missatges HELLO fent-se passar per un altre node.
- Un node que reenvia missatges de control alterats.
- Un node que no reenvia missatges requerits pel protocol.
- Un node que reenvia missatges de control broadcast sense alterar, però no reenvia el tràfic de dades unicast.

Un node reproduïx tràfic de control prèviament captat des d'un altre node. Com a contramesura es pot utilitzar l'autenticació del node origen per a missatges de control (per a la situació 2, 4 i 5) i dels enllaços individuals anunciats en els missatges de control (per a la situació 1 i 3). Tanmateix, per impedir als nodes repetir informació vella (i correctament autenticada) també s'exigeix informació temporal, permetent a un node identificar positivament tals missatges retardats.

L'OLSR és altament vulnerable als atacs de denegació de servei. Un atacant podria llançar paquets d'OLSR que continguessin informació falsa en grans quantitats. Això podria conduir a una situació on el procés de totes les dades podria saturar tots els recursos dels nodes de recepció, deixant-los incapaços de realitzar altres tasques. Finalment el servei d'OLSR podria caure deixant indisponible el node. Els mecanismes d'integritat poden impedir a un node realitzar tal atac, deixant-lo sense accés a la clau utilitzada.

Per tal de solucionar tots aquests problemes d'integritat, es va desenvolupar una extensió anomenada Secure OLSR. Aquesta extensió permet firmar tots els paquets pertanyents al protocol per a evitar els atacs exposats anteriorment.

Així doncs, la finalitat d'aquest escenari és testejar aquesta extensió i comprovar la viabilitat de ser utilitzat en els equips de què disposem. L'escenari és el mateix que el primer, a diferència que en aquest es fa ús de l'extensió de seguretat del protocol.

3.5. Quart escenari amb OLSR: rutes alternatives

En aquest apartat es pretén estudiar la capacitat del protocol de crear rutes alternatives i quins són els usos que se'n poden donar. Els usos que es

pretenen estudiar són: a mode de backup, per a si una ruta principal deixés d'estar disponible, i el balanceig de càrrega entre dues rutes.

- Funcionament bàsic del càlcul de rutes en OLSR:

El protocol OLSR manté informació dels altres nodes de la xarxa i construeix un mapa de la tipologia de la xarxa. Aquest mapa es guarda en una base de dades on cada entrada és un node, el qual té assignada una mètrica depenent de l'estat de la ruta. Aquesta mètrica s'assigna a cada ruta en funció del cost per a arribar al node. Aquesta taula s'actualitza cada vegada que es produeix una modificació en l'enllaç, en el veí, en el veí a dos salts o en la topologia de la xarxa.

ETX (Expected Transmission Count) és una extensió del protocol OLSR desenvolupada pel Massachusetts Institute of Technology. Aquesta extensió és un mecanisme que assigna a cada enllaç un valor sobre la qualitat de l'enllaç. Aquest valor es calcula mitjançant una tècnica d'enviament de paquets per l'enllaç i recompte dels paquets perduts.

El valor ETX és el nombre de intents de transmissió necessaris per a que un paquet aconsegueixi arribar al destí. Per a una xarxa ideal, aquest valor és 1 (cap paquet perdut). El valor ETX es calcula mitjançant la fórmula següent:

$$ETX = \frac{1}{NLQ \cdot LQ} \quad (3.1)$$

LQ (qualitat del enllaç) és el percentatge de paquets enviats i no perduts, expressats amb un número entre 0 i 1. NLQ és el mateix paràmetre però des del punt de vista del destí.

ETX proporciona la qualitat de la ruta, i no només el nombre de salts de la ruta. Aquest aspecte és molt important en les xarxes sense fils per les característiques que li donen al medi utilitzat.

Per a cada node podem tenir varies rutes, com es pot veure en el següent exemple de topologia:

Destination IP	Last hop IP	LQ	ILQ	ETX
10.224.0.1	10.224.0.5	0.76	0.60	2.20
10.224.0.1	10.224.0.6	0.10	0.21	49.08
10.224.0.1	10.224.1.12	0.07	0.22	68.30

Es pot observar que, per arribar a la adreça 10.224.0.1, ho podem fer passant per la IP 10.224.0.5, 10.224.0.6 o per la 10.224.1.12. Per tant en el cas que es produís un canvi en la topologia de la xarxa que impedís arribar a un node per una de les rutes, el protocol tornaria a calcular les rutes mitjançant els missatges TC. Un cop recalculades totes les rutes fins a un node, es podria seguir operant amb la ruta que millor mètrica oferís.

- Ús de backup de les rutes alternatives.

Com s'ha pogut veure, el funcionament del protocol proporciona un ús de backup de rutes a les rutes alternatives cap a un node. L'objectiu de l'escenari és provar aquesta característica. Per a fer això es munta un escenari compost per 4 nodes. En aquest escenari, el node A ha de comunicar-se amb el node D. Per a fer això, el node A disposa de dues rutes, la primera a través del node B i l'altre a través del node C.

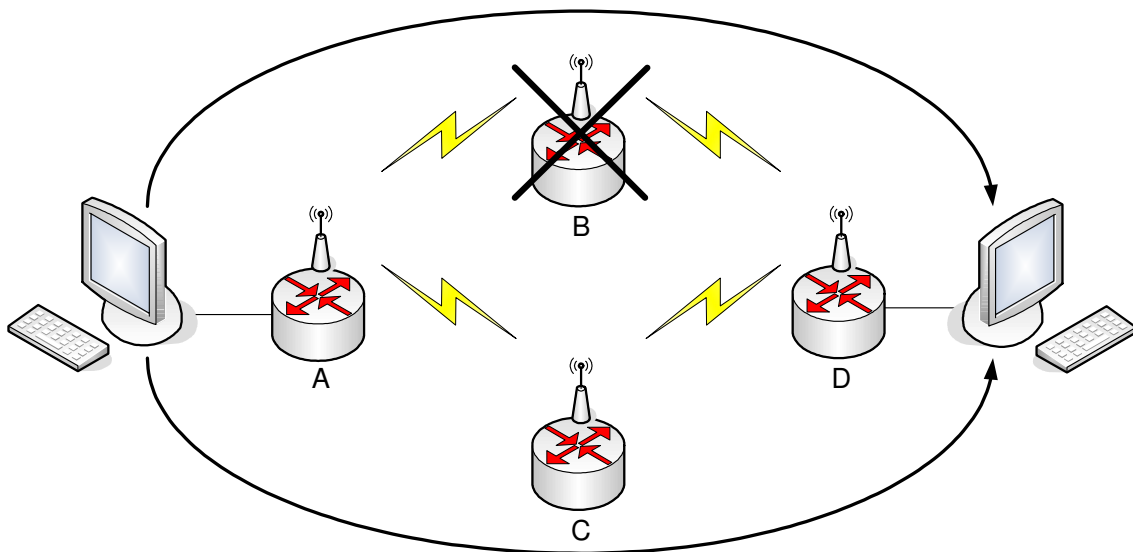


Fig. 3.3 Escenari de rutes alternatives com a backup

En posar en marxa l'escenari, el node A tria com a MPR a el node B i crea dues rutes cap al node D, una a través de B i l'altre a través de C. La qualitat de la ruta per B és millor i, per tant, comença a transmetre la informació a través de B. Per a provar la funcionalitat del escenari fem que el node B caigui, eliminant el camí que utilitzava per a transmetre. Aleshores el valor ETX de la ruta utilitzada augmenta, ja que perd tots els paquets que envia. El valor ETX de l'altra ruta es manté inferior al de la primera ruta i el protocol decideix començar a transmetre a través del node C. Passat el timeout del Hello, la xarxa elimina la ruta a través del node B, ja que ha quedat inaccessible.

A continuació es poden observar les taules d'encaminament fruit de l'experiència pràctica:

Node A: 192.168.1.1
 Node B: 192.168.1.2
 Node C: 192.168.1.3
 Node D: 192.168.1.4

Taula de rutes inicial:

Destination	Gateway	Metric	ETX	Interface
192.168.1.2/32	192.168.1.2	1	2.35	eth1
192.168.1.3/32	192.168.1.3	1	3.685	eth1
192.168.1.4/32	192.168.1.2	2	4.709	eth1

Taula de rutes després d'eliminar el node B:

Destination	Gateway	Metric	ETX	Interface
192.168.1.3/32	192.168.1.3	1	3.719	eth1
192.168.1.4/32	192.168.1.3	2	5.886	eth1

- Ús de balanceig de càrrega amb les rutes alternatives.

Un altre ús més avançat que es pot donar a les rutes alternatives és el balanceig de càrrega. El balanceig permet repartir el trànsit cap a un node en les diferents rutes que disposa. El criteri de balanceig pot ser des de dividir un tràfic molt gran cap a un node en dues rutes, per evitar saturar un enllaç (tenint-ne un sense utilització), fins a repartir el trànsit entre les diferents rutes, tenint en compte la tipologia del trànsit.

L'objectiu del següent escenari és aconseguir testejar aquest ús de les rutes alternatives. Per a això el següent escenari consta d'un node A, el qual ha de transmetre cap a una xarxa externa (en aquest cas Internet), però a una alta velocitat que no li pot proporcionar una sola porta d'accés a Internet. Per tant, l'objectiu d'aquest escenari és que aquest node utilitzi simultàniament les dues portes C i D, balancejant la càrrega per a accedir a Internet.

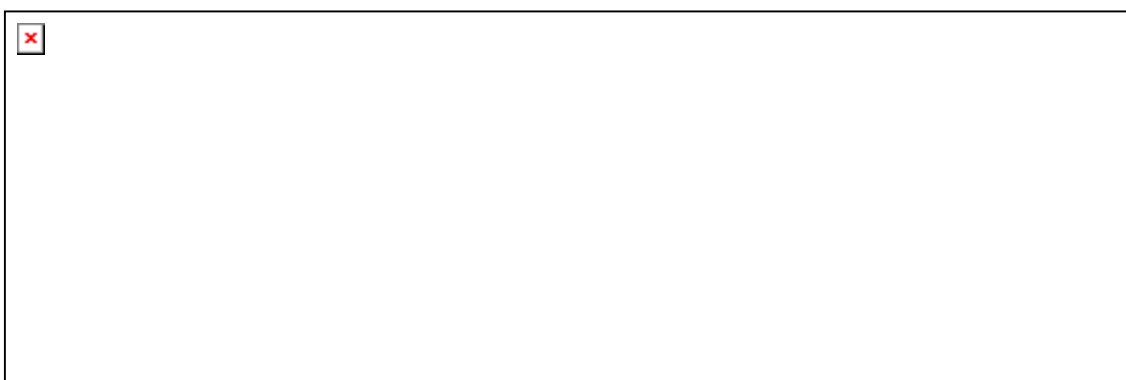


Fig. 3.4 Escenari de rutes alternatives per al balanceig de càrrega

Al realitzar el muntatge d'aquest escenari, el node A tria com a porta d'accés a Internet la porta B, ja que és la porta amb una millor mètrica, i comença a transmetre únicament per aquesta porta. El node A té un consum molt elevat cap a la xarxa externa, la qual cosa fa que la utilització d'una sola porta a aquesta xarxa sigui insuficient, creant la necessitat de poder utilitzar dues portes alhora. La solució a aquest problema és la utilització de túnels virtuals

per la xarxa. Aquests túnels anirien des del node A cap als nodes que tinguessin accés a Internet.

Per aconseguir aquest escenari, s'utilitza OpenVPN per a crear dos túnels ($A \rightarrow B$ i $A \rightarrow C$). Amb aquest pas s'aconsegueix que el node A tingui dos túnels contra diferents gateways. Per aconseguir que el node A balancegi la càrrega entre els dos túnels s'utilitzen les propietats d'`iproute2` que incorpora Linux.

3.6. Cinquè escenari: B.A.T.M.A.N.

En aquest apartat es pretén estudiar les millores introduïdes per l'algoritme B.A.T.M.A.N., un protocol creat per a arribar a ésser un dia el substitut de l'OLSR. El problema amb els protocols clàssics d'encaminament és que no es troben correctament adaptats a les característiques de les xarxes sense fils. L'OLSR, el protocol més utilitzat en aquestes tipus de xarxes, ha patit una gran quantitat de modificacions des de l'especificació original, per tal de superar els desafiaments imposats per les comunitats de xarxes sense fils mallades. Tanmateix, el creixement constant de la comunitat existent i el requisit del protocol de recalculer tota la topologia de la xarxa (sobretot en sistemes incrustats amb unes CPU poc potents, com els utilitzats en aquest estudi) ha esdevingut un problema per al protocol, ja que s'ha vist que no és suficientment escalable. Un exemple d'aquesta problemàtica és la xarxa alemanya Freifunk amb més de 450 nodes. Un node d'aquesta xarxa pot tardar uns quants segons en fer-ho si es tracta d'un sistema incrustat.

L'estratègia de millora del algoritme B.A.T.M.A.N. és dividir la informació sobre les millors rutes extrem a extrem entre els nodes de la malla entre tots els nodes participants. Cada node només rep i manté la informació sobre el millor veí per arribar a cada node. Tanmateix, la necessitat de tenir un coneixement global sobre els canvis locals esdevé innecessari. A més un mecanisme d'inundació a partir d'esdeveniments, però amb límit de temps prevé, de l'acumulació d'informació de topologia contradictòria (una raó molt possible per a l'existència de bucles d'encaminament) i limita la quantitat de missatges de topologia que inunden la xarxa (evitant així una excessiva despesa de recursos de control de tràfic). L'algoritme està dissenyat per a xarxes on els enllaços no són gaire fiables.

Aquest escenari és idèntic al primer però, en aquest cas, utilitzant el protocol B.A.T.M.A.N. per a l'encaminament. Per tant, els objectius d'aquest escenari són l'estudi del funcionament bàsic d'una xarxa sense fils amb el protocol B.A.T.M.A.N. i la realització d'una comparació entre B.A.T.M.A.N. i OLSR. La xarxa està formada per tres encaminadors sense fils amb el protocol OLSR. En un d'ells penja un ordinador personal i en un altre es té connexió a Internet.

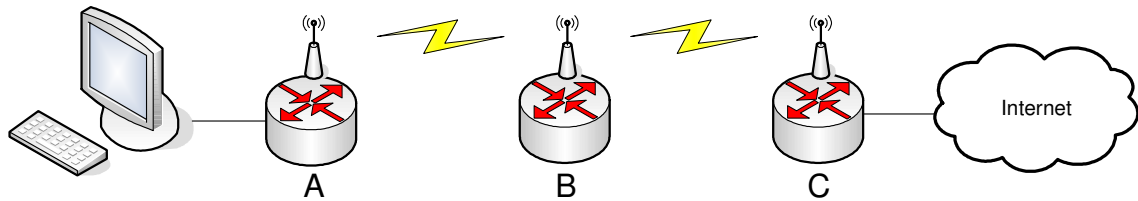


Fig. 3.5 Escenari amb B.A.T.M.A.N.

Aquest escenari ha permès demostrar el funcionament del protocol que des del punt de vista d'un usuari és molt similar a OLSR.

Realitzant un ping a un lloc web d'Internet podem comprovar que el protocol funciona correctament encaminant els paquets entre tots els nodes intermitjos:

```
C:\Documents and Settings\David Serra>ping www.google.es
```

```
Haciendo ping a google.navigation.opendns.com [208.69.34.230] con 32 bytes de datos:
```

```
Respuesta desde 208.69.34.230: bytes=32 tiempo=79ms TTL=253
Respuesta desde 208.69.34.230: bytes=32 tiempo=78ms TTL=253
Respuesta desde 208.69.34.230: bytes=32 tiempo=79ms TTL=253
Respuesta desde 208.69.34.230: bytes=32 tiempo=79ms TTL=253
```

```
Estadísticas de ping para 208.69.34.230:
```

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

```
Tiempos aproximados de ida y vuelta en milisegundos:
```

```
Mínimo = 78ms, Máximo = 79ms, Media = 78ms
```

En l'annex 2 es pot trobar un petit anàlisi de càrrega de CPU del node B d'aquest escenari. En aquest anàlisi es pot observar que la càrrega de CPU és molt baixa donat que el nombre de nodes de l'escenari és molt petit. És interessant comparar aquest anàlisi al ja realitzat en el escenari 1 amb OLSR, on la càrrega de CPU és una mica inferior a la càrrega utilitzada per B.A.T.M.A.N. En ser escenaris amb un nombre de nodes tan baix, no es pot afirmar ja que OLSR consumeix menys recursos que B.A.T.M.A.N. Per a poder fer una petita comparació entre l'escalabilitat d'ambdós protocols, en el següent punt es realitza una simulació de dues xarxes idèntiques utilitzant un protocol d'encaminament diferent.

3.6.1. Millores introduïdes per B.A.T.M.A.N envers OLSR

Emmarcat dins del projecte OLSR-NG, el grup de desenvolupament de B.A.T.M.A.N. ha realitzat proves per tal de comparar a la pràctica les millores introduïdes pel protocol en comparació amb l'estàndard OLSR.

En la figura 3.6 es mostra la comparació de càrrega de CPU en funció del nombre de veïns per cada node entre tots dos protocols. L'últim valor (6,5) d'OLSR ha estat omès, ja que els nodes estaven completament saturats. La mesura es va realitzar per a un valor constant de 60 nodes. En aquesta figura es pot observar que el protocol OLSR no respon gaire bé a un augment significatiu de nodes, disparant-se el seu consum de CPU. En el cas de B.A.T.M.A.N., es pot observar un augment de CPU molt més controlat amb un pendent de 0,2.



Fig. 3.6 **Consum de CPU en funció del nombre de veïns per node**

La figura 3.7 mostra la càrrega de CPU en funció del nombre de nodes en la xarxa. Com es pot observar al gràfic, per a xarxes amb pocs nodes, el protocol OLSR consumeix menys CPU. Aquet fet s'inverteix quan el nombre de nodes supera el valor aproximat de 62 nodes. A partir d'aquest punt, el consum de CPU del protocol OLSR es dispara en comparació amb el consum de B.A.T.M.A.N.



Fig. 3.7 **Consum de CPU en funció del nombre de nodes**

CAPÍTOL 4. APLICACIÓ A GUIFI.NET

4.1. Introducció

L'objectiu d'aquest capítol és la redacció d'una proposta de disseny per a GUIFI.NET. Aquest nou disseny es basa en una xarxa de petites xarxes, cada una de les quals és una zona OLSR. Aquestes zones OLSR es comuniquen utilitzant portes d'enllaç cap a la resta de la xarxa mitjançant un backbone el qual pot estar format per múltiples tecnologies. Algunes d'elles poden ser des d'enllaços ràdio, com els també utilitzats dins de cada subxarxa, fins a túnels a través d'Internet, que proporcionarien la capacitat d'ampliar la xarxa a un territori molt més extens.

S'ha vist que el disseny actual de GUIFI.NET no és sostenible i la proposta que es realitza en aquest estudi ha de ser robusta i escalable al gran creixement que està experimentant la comunitat. A l'hora de definir aquesta proposta s'ha decidit dividir-la en dues parts. La primera part correspon al disseny de cada una de les subxarxes que utilitzen OLSR com a protocol d'encaminament intern, la qual inclou la gran majoria d'equipament que conforma la infraestructura de GUIFI.NET. A continuació, en la segona part es descriu la utilització d'un backbone per a la interconnexió d'aquestes subxarxes entre si i fins i tot amb altres xarxes externes a GUIFI.NET. Aquesta segona part inclou els equipaments anomenats supertrastos per a la creació d'aquesta estructura d'interconnexió.

Finalment es troba una nota aplicable a la implantació d'aquesta o qualsevol altra reforma de Guifi.net. Tot procés de migració és altament costós i delicat i, per tant, ha d'estar degudament planificat i executat.

4.2. Disseny de la xarxa d'accés

En aquest punt es realitza un conjunt de recomanacions per a dur a terme una correcta configuració de la xarxa, les quals són fruit d'aquest estudi en el disseny i la planificació de xarxes i de la posterior aplicació a Guifi.net. Aquesta xarxa és la que proporciona l'accés als usuaris a la xarxa GUIFI.NET. Aquí s'inclou la gran majoria d'equipament que conforma la infraestructura. La idea d'aquesta proposta és definir el disseny d'una xarxa sense fils orientada a una filosofia de xarxa amb més mobilitat, però sense deixar de banda altres aspectes tan importants com l'escalabilitat que ha de tenir una xarxa amb un factor de creixement tan elevat com té Guifi.net.

Configurar els nodes en arquitectura ad-hoc en lloc de l'arquitectura d'infraestructura, fins ara utilitzada, permet distribuir la càrrega del tràfic de la xarxa en tots els nodes que hi intervenen i eliminar el problema que tota una subxarxa depengui d'un punt d'accés de cara a possibles fallades d'aquest. Per

a la gestió de l'encaminament de la xarxa es fa necessària la utilització d'un protocol d'encaminament, ja que sense aquest un node no podria accedir a un altre node de la xarxa per al qual no tingués una comunicació directe.

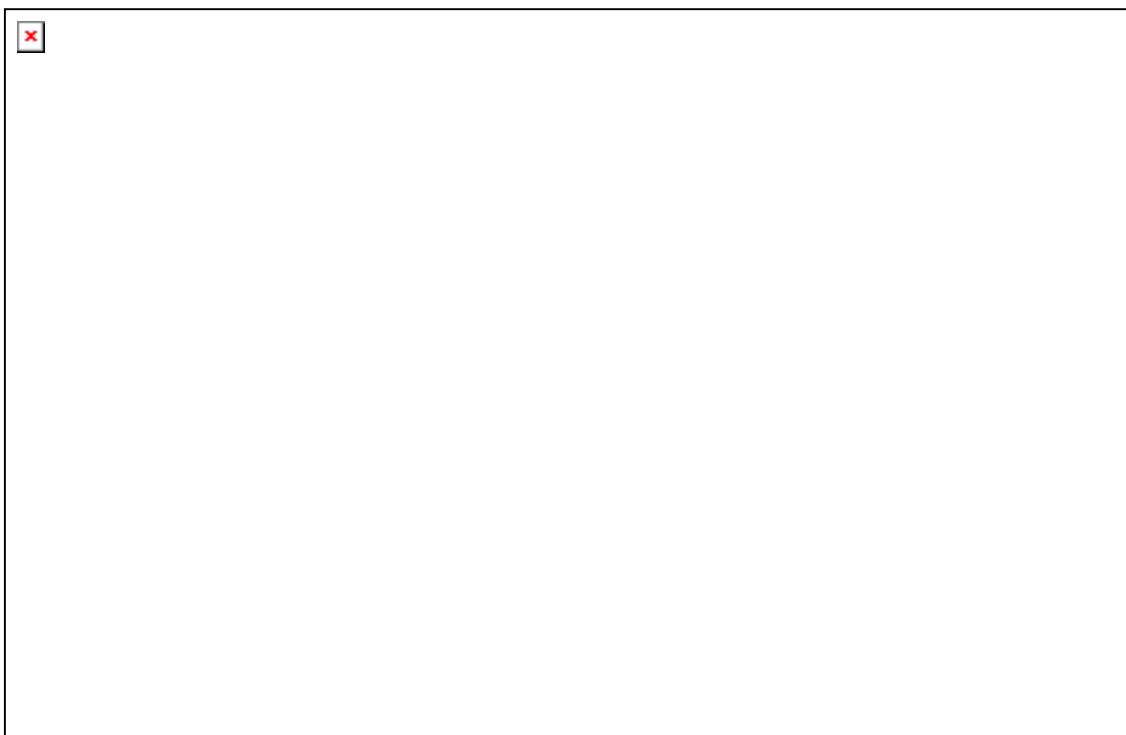


Fig. 4.1 Disseny d'una zona OLSR de la xarxa d'accés

Donades les anteriors premisses, el protocol que millor s'adapta a la proposta de disseny és l'OLSR. Aplicar aquest protocol a la xarxa proporciona la mobilitat necessària per a terminals portàtils o equips de butxaca, ja que si es mou dins de l'àrea de cobertura de qualsevol altre dispositiu de la xarxa, sempre disposarà d'accés a tota la resta de nodes i de manera completament transparent per a l'usuari. L'OLSR és un protocol idoni per a xarxes amb unes característiques que fan que altres protocols no siguin recomanables. Aquestes característiques són, per exemple, nuclis de població en què hi ha una densitat elevada d'usuaris o una orografia del terreny complicada que fa que les comunicacions via ràdio siguin bastant inestables.

Fins ara s'han descrit alguns avantatges sobre la utilització d'OLSR, però també hi ha inconvenients. Tal com s'ha pogut veure en el cinquè escenari del tercer capítol, l'OLSR no és gaire escalable. Per a xarxes on el nombre de nodes és gran, el consum de CPU dels nodes augmenta de manera significativa i és un problema més significatiu el fet que la majoria d'equipaments de Guifi.net siguin dispositius embotrats amb unes CPU bastant limitades. Per tant, l'aplicació d'OLSR a tota la xarxa és del tot inviable ja que deixaria de ser escalable i, fins i tot amb el nombre actual de nodes de què

disposa Guifi.net, la xarxa estaria completament col·lapsada. D'aquí neix la idea d'aquesta proposta de dividir tota la xarxa en petites subxarxes, aconseguint les millores que aporta l'OLSR però millorant-ne l'escalabilitat.

Tot i que, com s'ha pogut veure en el capítol 3, el B.A.T.M.A.N. és un protocol que aporta certes millores a l'OLSR, (per exemple l'escalabilitat pel disminuït ús de CPU dels nodes) s'ha triat aquest segon donat que a dia de realitzar aquest estudi, el B.A.T.M.A.N. és un protocol que encara es troba en desenvolupament. Aquest fet fa que no existeixi un estàndard i que existeixin múltiples implementacions, la majoria de les quals encara no són del tot estables. A diferència del B.A.T.M.A.N., l'OLSR ja disposa d'un RFC (RFC3626) i les versions de les implementacions són estables en la seva majoria.

Utilitzant l'OLSR s'aconsegueix mobilitat dins de la subxarxa on es trobi el node, però no entre diferents subxarxes OLSR. En aquest cas un node que es mogui entre diferents zones OLSR haurà de reconfigurar en el dispositiu l'ESSID i el canal ràdio, en el cas de que difereixin, i l'adreçament assignat a part del tall de connectivitat associat a tot el temps en què es tarda en modificar aquests paràmetres. Una manera de minimitzar les molèsties ocasionades pel canvi de zona d'OLSR pot ser la utilització d'un servidor d'adreces DHCP. Aquest servidor d'adreces podria estar allotjat en el mateix dispositiu que realitzarà la tasca de porta d'accés cap a la resta de les subxarxes atès que, per les seves característiques, aquest node ha de ser un node bastant estable i sempre actiu. Introduir aquesta característica a les xarxes OLSR per a l'assignació d'IPs dintre d'una zona ajuda a una correcta gestió de les IP i a facilitar la tasca dels usuaris en configurar els terminals. A més també es facilita la configuració en cas que canviï de subxarxa, ja que l'usuari no ha de saber quin adreçament disposa cada zona aportant una certa mobilitat entre les diferents zones, fent que el canvi de zona gairebé sigui transparent per a l'usuari.

Per al correcte funcionament de la xarxa és molt recomanable que com a veí sempre es trobi un node fix, sobretot en densitats de població disminuïdes. La fiabilitat que proporciona un enllaç a un node fix envers un de mòbil és molt més elevada. Per a aconseguir això, en el procés de creació de la xarxa OLSR es recomana la instal·lació d'un conjunt de ràdios fixes i amb connectivitat entre si. Aquestes ràdios estarien esteses per tot el territori que es vol cobrir per la zona OLSR i podrien ser d'un abast superior al que ofereix un node qualsevol. No és necessari que aquest conjunt de nodes es disposin en forma de xarxa completament mallada, ja que OLSR ja encamina els paquets cap als nodes no veïns i la configuració d'aquests nodes seria la mateixa que la resta de dispositius. Aquesta recomanació permet l'existència d'una xarxa base fixa i bastant estable sobre la qual els usuaris puguin utilitzar els seus dispositius mòbils.

Tots els dispositius que desitgin tenir connectivitat amb la totalitat d'una zona OLSR tenen la necessitat de tenir activat el protocol d'encaminament d'OLSR. Si aquesta premissa no es compleix, un dispositiu tan sols podria arribar als dispositius que té al abast, ja que la resta de dispositius no tenen informació

sobre aquest. Una solució per a dispositius que no disposin d'aquest protocol és la creació de subxarxes que penguin d'un node que sí disposa d'aquest protocol. Aquesta subxarxa tindria d'estar anunciada a través del node de què penja mitjançant la utilització de la funció HNA. Aquesta solució també és aplicable a usuaris que disposin d'una xarxa privada amb diferents màquines i que vulguin tenir connectivitat per a aquestes màquines. En cas que no es disposés d'adreçament per a aquestes subxarxes o bé es volgués conservar un adreçament privat, una altra solució podria torbar-se en la utilització d'un NAT en el dispositiu d'interconnexió amb la zona OLSR.

Els paràmetres de configuració de cada zona OLSR no tenen motiu per a ser idèntiques. El funcionament correcte d'una zona OLSR depèn d'una configuració ajustada als factors de l'indret . Així doncs, alguns d'aquests factors són l'orografia del terreny, les condicions mediambientals de la zona, la densitat de nodes, la mobilitat requerida pels usuaris, etc.

L'OLSR és un protocol que s'adapta molt bé a condicions orogràfiques complexes en comparació a altres protocols, però s'ha de tenir en compte que tot i que el protocol d'encaminament funcioni bé, les transmissions entre aquests nodes tindran una taxa d'errors superiors i això provocarà un alentiment de la xarxa. Per tant, augmentar el nombre de nodes de la xarxa o subdividir la zona en zones més petites pot ser la solució d'aquest problema.

Quant a la densitat de la xarxa, l'OLSR està pensat per a xarxes amb una densitat elevada, però un excés d'aquesta densitat pot conduir a la xarxa a un alentiment generalitzat. Contràriament, una disminució d'aquesta densitat pot provocar que les rutes entre dos nodes siguin mínimes o nul·les en alguns casos. Aquest problema podria causar dificultats per a trobar rutes entre extrems de la xarxa o inclús dividir la xarxa de manera que un tros de la zona deixés de tenir connectivitat amb la resta de la zona. La solució d'ambdós problemes es troba en dividir la zones en més zones. D'aquesta manera, per a una densitat elevada podem crear diferents zones utilitzant diferents canals per als nodes de cada zona. Això ens proporcionaria disminuir la densitat de cada zona. L'OLSR és un protocol amb problemes per a les xarxes amb un nombre bastant elevat de salts. Per a zones on la densitat es vegi molt disminuïda a causa d'una àrea de terreny per cobrir molt elevada, el fet de dividir l'àrea en varies zones i interconnectar-les totes mitjanant la xarxa de backbone, aportaria una millor connectivitat dins de cada zona i es deixaria en mans de la xarxa de backbone la correcta connectivitat entre les zones OLSR.

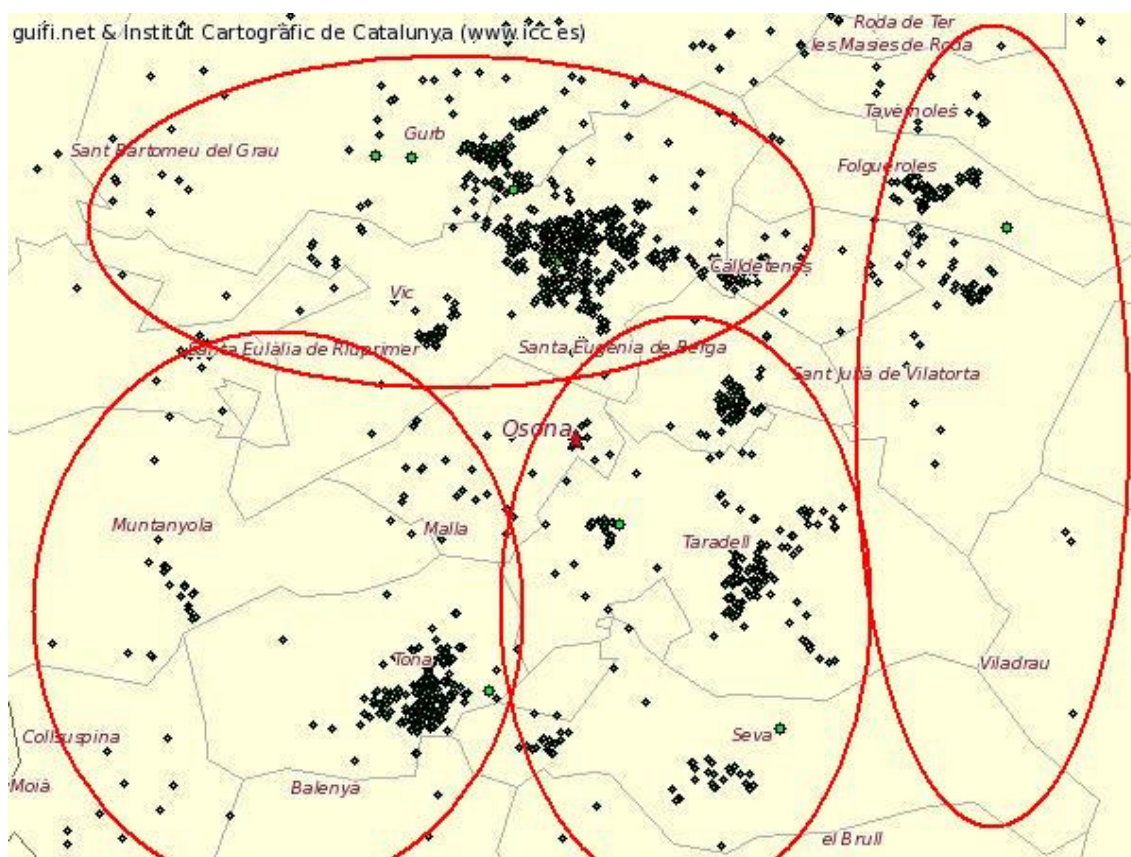


Fig. 4.2 Exemple de disseny del particionat en zones de l'àrea de Vic de la comarca d'Osona

Tal i com s'ha fet referència a la grandària de les diferents zones OLSR, també és considera interessant no fixar uns valors estables per als paràmetres que ofereix el protocol. Per tant és recomanable ajustar els valors d'interval de Hello, MID, HNA i TC a les característiques de la zona OLSR. Ajustant bé aquests paràmetres es podrà aconseguir una xarxa més estable. Totes aquestes recomanacions depenen de les característiques de l'àrea que s'ha de cobrir i són molt complexes de fixar. Per tant, tot el disseny en concret de cada zona OLSR ha de ser fruit d'un estudi adequat de l'àrea i a continuació d'una experiència sobre la mateixa xarxa per anar ajustant les configuracions a mesura que la xarxa és utilitzada.

Es recomana la utilització del protocol DHCP per a l'assignació d'IP dintre d'una subxarxa per a una correcta gestió de les IP i per a facilitar la tasca dels usuaris en configurar els terminals ja que no s'ha de saber quin és l'adreçament de cada subxarxa. Amb això es permet certa mobilitat entre les diferents subxarxes sent gairebé transparent a l'usuari.

Per a subxarxes amb unes característiques elevades de trànsit extern a la zona OLSR o inclús per a la necessitat de sortides de backup de la zona OLSR, existeix la possibilitat de configurar més d'un node de porta d'accés a la resta de la xarxa. Aquesta configuració es pot aconseguir mitjançant la configuració

del paràmetre HNA de tots els nodes que es vulguin per a realitzar aquesta tasca. Aquests nodes tindrien d'oferir connectivitat a la resta de la xarxa en aquest paràmetre. Cada node dins d'una zona OLSR utilitzaria el node a una distància inferior per a sortir de la zona OLSR en el cas d'una configuració estàndard. També existeix la possibilitat de configurar un node mitjançant la utilització de túnels per a que utilitzés ell sol més d'una porta de sortida alhora, fet que ens proporcionaria un balanceig de càrrega d'un node cap al exterior d'aquesta zona. Aquesta configuració seria adequada per a nodes amb una alta necessitat de consum de recursos d'amplada de banda.

4.3. Disseny de la xarxa de distribució

En aquesta proposta es considera la idea de veure GUIFI.net com una xarxa dividida en vàries subxarxes. Aquestes subxarxes, pertanyents a la xarxa d'accés, són les diferents zones OLSR o inclús altres subxarxes que per característiques de la mateixa xarxa s'hagi escollit utilitzar un altre protocol. Per tant la xarxa que es descriu en aquest punt és el nus de comunicacions que proveirà connectivitat entre totes les subxarxes de GUIFI.net. Tal com s'ha comentat anteriorment, el motiu per escollir un model basat en una xarxa de subxarxes ha estat els conjunt de problemes d'escalabilitat que aportaria una xarxa amb una única zona OLSR per a la quantitat de nodes, rutes i la difícil adaptació del protocol OLSR a xarxes amb un nombre elevat de salts entre nodes, tenint en compte les baixes característiques tècniques de la majoria de dispositius utilitzats en aquesta xarxa.

Per al disseny d'aquesta xarxa s'ha de tenir en compte que són nodes que donen servei a un nombre elevat d'usuaris i que, per tant, els requeriments tècnics dels nodes han de ser més elevats que la resta de nodes de les zones OLSR. En tractar-se d'una xarxa de distribució, l'arquitectura escollida és una xarxa mallada. Aquesta elecció ens proporciona una protecció envers desastres millor que la proporcionada per altres arquitectures.

Per a aquests nodes es poden utilitzar els anomenats supertrastos, routers que han de disposar de múltiples interfícies de xarxa. Una per a connectar a la xarxa de d'accés i les demés per a interconnectar amb la xarxa de distribució. Donat que aquests nodes són els que componen la xarxa de distribució, han de ser més fiables que no pas la resta de nodes per a proporcionar l'estabilitat necessària del conjunt de la xarxa. Un altre motiu per a disposar de portes d'accés amb unes característiques tècniques més elevades que la resta de dispositius és la possibilitat d'utilitzar aquest dispositiu per a allotjar diferents serveis per a la gestió de la subxarxa com pot el servidor d'assignació d'adreces DHCP.



Fig. 4.3 Disseny de la xarxa de distribució

Quant a la configuració de la interfície que proporciona connectivitat cap al costat de la xarxa d'accés, difereix de la resta de nodes per la configuració del paràmetre HNA per a fer que aquest informi de la resta de subxarxes.

En aquesta proposta es vol que la xarxa de distribució estigui oberta a les característiques necessàries per a realitzar els enllaços. Així doncs, es vol que aquesta xarxa permeti la utilització de diferents tecnologies d'enllaç. Algunes d'aquestes tecnologies poden ser enllaços ràdio estàndards de 802.11b/g o bé altres tecnologies, com enllaços ràdio a 5Ghz, que proporcionarien enllaços fixes a zones allunyades amb una visibilitat directe, línies utilitzant cable o fibra òptica per a enllaços de gran capacitat, o fins i tot túnels a través d'Internet que ens proporcionarien fer créixer la xarxa arreu on hi hagi disponibilitat d'Internet, sense importar la distància de les zones.

Per a la gestió d'aquesta xarxa de distribució, tenint en compte que es tracta d'una xarxa amb enllaços molt més fiables que a la xarxa d'accés, es recomana la utilització d'un protocol d'encaminament adequat a les característiques de la

xarxa com pot ser l'OSPF. Només seria necessari executar aquest protocol d'encaminament en els nodes de la xarxa de distribució, ja que aquests ja proporcionen connectivitat a la resta de nodes de la xarxa d'accés. És interessant observar que les taules d'encaminament d'aquest protocol no creixerien d'una manera desproporcionada, ja que només augmentarien en relació al nombre de xarxes OLSR. En el cas hipotètic que el creixement fos tan elevat que el protocol d'encaminament no permetés un encaminament de manera correcte, o bé es requereix la interconnexió de la xarxa GUIFI.net amb altres xarxes, la solució podria trobar-se en la utilització d'un protocol d'encaminament extern, com pot ser el BGP.

4.4. Implicacions d'implantació

Qualsevol procés de migració entra en seriosos dubtes sobre el seu desenvolupament ideal. La migració que comporta la proposta realitzada és costosa i, tot i que existeixen recomanacions de metodologia a seguir per a realitzar migracions semblants, no existeix una solució universal que es pugui seguir al peu de la lletra podent confiar en que es completarà sent un èxit rotund.

Per a que la migració pugui esdevenir un èxit es recomana una planificació llarga i detallada de tot el procés. S'ha de tenir en compte que cada zona OLSR és diferent i que, per tant, sorgeix la necessitat de realitzar una planificació específica per a cada zona. Un cop realitzada la planificació adequada i tenint en compte el màxim nombre de successos que poden sorgir durant la migració, és molt recomanable realitzar una simulació de la xarxa abans de la implementació en la plataforma en producció. Per a finalitzar, durant el procés de migració se n'haurà de realitzar un seguiment per a determinar si el procés s'està desenvolupant tal com s'havia establert en la planificació.

La proposta realitzada implica una modificació gairebé total de la infraestructura de la xarxa i s'ha de recordar que GUIFI.net és una xarxa d'unes dimensions bastant elevades. Per tant, es recomana realitzar aquest procés dividit en diferents fases i utilitzar tecnologies que permetin, en la mesura del possible, la migració, com per exemple firmwares que permetin operar tant amb el protocol que cal substituir com amb el nou. D'aquesta manera es podrà aconseguir que el funcionament de la xarxa es vegi mínimament afectat. Les fases en què es poden dividir aquesta migració són, en un principi, la migració dels diversos conjunts de nodes cap a zones OLSR i, a mesura que es realitza aquesta, anar modificant l'arquitectura de la xarxa de distribució segons les necessitats de les zones OLSR.

CAPÍTOL 5. CONCLUSIONS

Durant aquest projecte s'ha estudiat la situació actual de la comunitat Guifi.net. Aquesta comunitat posa en comú tots els recursos dels seus individus sobre una infraestructura de comunicacions. Aquesta infraestructura és una xarxa sense fils oberta a tots els membres de la comunitat. Aquestes comunitats proporcionen als seus individus una independència per a poder seguir evolucionant, que només estan limitades per les limitacions tecnològiques i les ganes dels propis membres, mentre que d'altres tipus de xarxes de comunicacions comercials estan sotmeses a les limitacions de les estratègies comercials pròpies de les empreses. Les característiques pròpies d'aquest tipus d'infraestructura permeten la creació d'una xarxa de comunicacions a un cost inferior del de les xarxes tradicionals de les empreses de telecomunicacions. Actualment GUIFI.net compta amb més de 3.000 nodes i un índex de creixement molt elevat. Això fa que, tot i ser una xarxa distribuïda, es comencin a entreveure alguns problemes d'escalabilitat. Per tant, des d'un principi s'ha volgut realitzar una proposta de millora de la xarxa per pal·liar aquests problemes d'escalabilitat i proporcionar a la xarxa característiques avui inexistents, com la mobilitat.

Mitjançant les experiències pràctiques amb els diferents protocols, s'ha pogut comprovar el funcionament i la robustesa dels protocols, que proporcionarien les millores que cal introduir a la xarxa. Aquestes experiències pràctiques s'han realitzat mitjançant un escenari molt pròxim a la xarxa real, per exemple utilitzant el mateix maquinari que l'utilitzat actualment a Guifi.net. Per tant, les maquetes realitzades durant l'estudi pràctic es poden considerar a zones de Guifi.net. Tot i tenir en compte que, tractant-se d'una xarxa sense fils, necessita una configuració bastant específica per a adequar-se a les característiques de cada zona, posar en pràctica aquestes tecnologies, també ha permès obtenir les configuracions i valors de paràmetres dels diferents protocols, robustos i adequats per a una xarxa de les característiques de Guifi.net.

Com a última tasca dins d'aquest projecte, s'ha realitzat la redacció d'una proposta de millora basada en els resultats de les experiències pràctiques i les necessitats i característiques de Guifi.net. Aquesta proposta s'ha realitzat de tal manera que sigui el màxim escalable i permeti un creixement futur bastant elevat. Cal tenir en compte també que la proposta realitzada és bastant oberta i que permet que, en el moment d'una possible implantació real, es disposi d'una llibertat, així com realitzar nombroses recomanacions quant a la configuració final en funció de les necessitats particulars dels membres de la comunitat i de cada zona.

5.1. Impacte medioambiental

L'implantació de la proposta de millores sobre la xarxa realitzada només implica modificacions a nivell de software en els diferents equips i, per tant, el seu impacte ambiental és quasi inexistent. A més, no anima activament a la implantació de nous enllaços. L'avaluació d'impacte de l'utilització d'enllaços

radioelèctrics és fruit d'una gran polèmica sobre la seva afectació sobre la salut en els éssers humans, de la qual se n'han fet nombrosos estudis. Aquests estudis recolzen ambdós possibilitats sobre l'afirmació i la negació d'aquesta afectació sobre la salut i, per tant, requereixen un estudi bastant complex que aquest projecte no arriba a abastar. En el cas de la tecnologia 802.11, cal tenir present que les bandes lliures són d'ús obert a tota la població segons la normativa espanyola i que la seva utilització està regulada per la llei general de telecomunicacions de l'any 2003.

5.2. Línies futures d'estudi

Abans de finalitzar aquestes conclusions es vol oferir una llista de tasques que es poden iniciar dins de Guifi.net i, per tant, conformen les línies futures d'estudi per a la xarxa Guifi.net. La línia més immediata es basa en veure l'evolució del nou protocol B.A.T.M.A.N. amb noves implementacions i millores, així com si finalment esdevindrà un estàndard. Per últim, també cal estudiar l'aplicació que pot tenir en la millora de l'encaminament a nivell de la xarxa d'accés. Una altra d'aquestes futures línies d'estudi que es poden obrir per a la millora de la xarxa és la implementació de noves tecnologies d'enllaç, com el nou estàndard 802.11n que proporciona velocitats de transferència més elevades en entorns més desfavorables, o com el WiMAX (802.16 MAN) que es basa en la creació de MAN sense fils en comptes de LAN sense fils. Aquestes tecnologies s'han d'estudiar profundament i cal veure la seva aplicació a Guifi.net, ja que proporcionen grans millores, tot i que tenen certs inconvenients. Per exemple, WiMAX proporciona una extensió de cobertura més elevada a velocitats més altes, però els costos dels equips i la necessitat d'una llicència de radioenllaç per l'ús dependent de les freqüències utilitzades pot esdevenir un problema a l'hora de l'aplicació a Guifi.net.

5.3. Avaluació personal de l'estudi

Per a finalitzar aquestes conclusions es creu que l'avaluació del desenvolupament d'aquest estudi és positiu ja que els objectius proposats a la introducció s'han complert en haver aconseguit una proposta de millores funcionals sobre Guifi.net.

BIBLIOGRAFIA

- [1] Medina Santos, A., *Comparativa de los protocolos AODV y OLSR con un emulador de redes ad-hoc*, Treball Fi de carrera, Universitat Politècnica de Catalunya, Castelldefels (2006).
- [2] Vilajoliu Galceran, B., *Millora de la gestió d'una xarxa WiFi: Guifi.net*, Projecte Fi de carrera, Universitat Politècnica de Catalunya, Castelldefels (2006).
- [3] Clausen, T and Jacquet, P., *Optimized link state routing protocol (OLSR)*, Internet Engineering Task Force (IETF), rfc3626.txt, October 2003.
- [4] Roca, R., *Fent xarxa lliure sense fils*, (2004) URL: <<http://www.guifi.net>>
- [5] Tønnesen, A., *Implementing and extending the Optimized Link State Routing Protocol*, UniK University Graduate Center University of Oslo, (2004). URL: <<http://www.olsr.org>>
- [6] Neumann, A., Elektra Aichele, C. and Lindner, M., *B.A.T.M.A.N Status Report*, (2007) URL: <<http://open-mesh.net/B.A.T.M.A.N./doc/B.A.T.M.A.N.-status.pdf>>.
- [7] Ward, B., *The Linux Kernel HOWTO*, (2001) URL: <<http://www.linuxdocs.org/HOWTOs/Kernel-HOWTO.html>>
- [8] Charles E. Perkins, *Ad-hoc Networking*, Addison-Wesley Professional, Mountain View (2001).
- [9] Roman, J., "RF Safety and Risk Communications - The Wi-Fi industry perspective", Inter-American Telecommunication Commission, *InfoCitel*, 25 (2006)
- [10] Aaron and Bern, *OSLR-NG current status*, (2007) URL: <<http://wiki.funkfeuer.at/index.php/OLSR-NG>>
- [11] D. K. Kim, *A New Mobile Environment: Mobile Ad-hoc Networks (MANET)*, *IEEE Vehic. Tech. Soc. News*, August 2003.
- [12] Ruíz Martínez, P.M., *Arquitectura multicapa para ofrecer comunicaciones multidesfino eficientes en extensiones ad - hoc inalámbricas y móviles conectadas a redes ip fijas*, Universidad de Murcia, 2002.

ACRÒNIMS I SIGLES

ADCCP	Advanced Data Communication Control Procedures
B.A.T.M.A.N.	Better Approach To Mobile Ad-hoc Networking
BGP	Border Gateway Protocol
BSSID	Basic Service Set Identifier
CMT	Comisión del Mercado de las Telecomunicaciones.
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
EPSC	Escola Politècnica Superior de Castelldefels
ESSID	Extended Service Set Identifier
ETX	Expected Transmission Count
FTP	File Transfer Protocol
GPL	General Public Licence
HNA	Host and Network Association
HDLC	High-Level Data Link Control
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Acces Protocol
INRIA	Institut National de Recherche en Informatique et en Automatique
IP	Internet Protocol
IPv6	Internet Protocol versió 6
LAN	Local Area Network
LQ	Link Quality
LSA	Link State Advertisement
MANET	Mobile Ad-hoc Network
MID	Multiple Interface Declaration
MPR	MultiPoint Relays
NAT	Network Address Translation
NVRAM	Non Volatile RAM
OLSR	Optimized Link State Routing
OSPF	Open Short Path First
POP	Post Office Protocol
PPP	Point to Point Protocol
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request For Comments
RIP	Routing Internet Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
TC	Topology Control
TCP	Transport Control Protocol
UDP	User Datagram Protocol
UPC	Universitat Politècnica de Catalunya
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

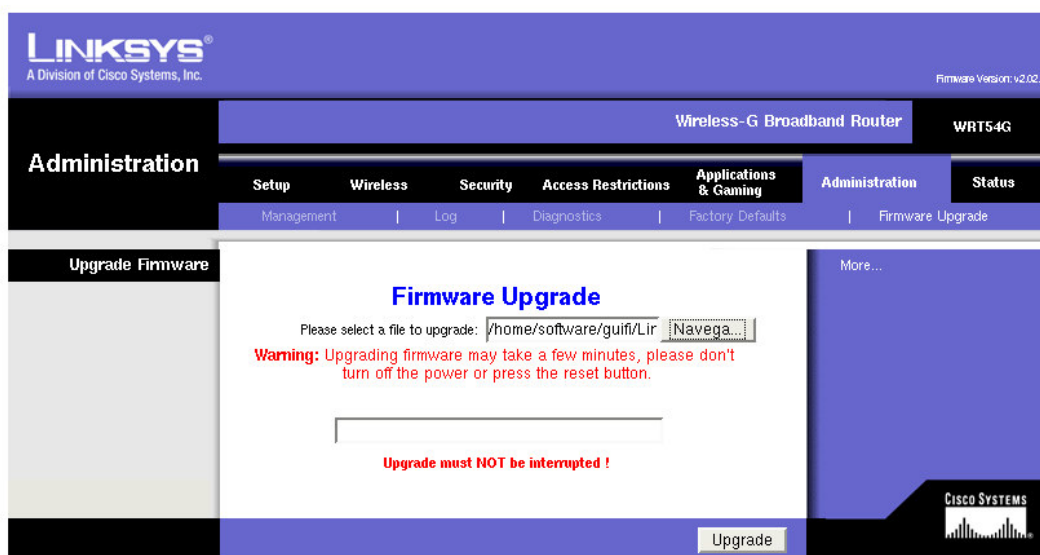
ANNEX 1: PREPARACIÓ DELS WRT54GL

A1.1. Introducció

L'objectiu principal d'aquest punt és mostrar els passos seguits per tenir els WRT54GL totalment funcionals per als escenaris a partir dels models adquirits al proveïdor. De la mateixa forma, tots els passos intermedis, o altres procediments que es consideren una transferència de coneixement, també es troben recollits en aquest punt. Per tant, els escenaris presentats al llarg del document han de poder reproduir-se fàcilment seguint aquestes pàgines.

Per al primer cop que es canvia el firmware dels WRT54GL es pot utilitzar el mètode via web. El WRT54GL permet pujar-li un firmware des de la interfície ASP del web. Els passos per a realitzar el canvi del firmware són els següents:

- Arrencar el WRT54GL.
- Arrencar un PC i connectar-lo a un dels ports del switch del WRT54GL.
- Configurar la targeta de xarxa del PC a la IP 192.168.1.2.
- Utilitzar un navegador web i connectar-se a <http://192.168.1.1/>.
- A continuació ens hem d'autenticar. (Paraula de pas per defecte: admin, usuari en blanc).
- Escollir l'opció Upgrade Firmware del menú Administration.
- Seleccionar al firmware la ruta on es trobi el firmware que s'ha de pujar.
- Prémer Upgrade.
- Esperar uns 2 minuts.



- Un cop s'hagi actualitzat el firmware correctament, apareixerà el missatge "Upgrade are successful".

Per a flashear els WRT54GL les pròximes vegades és necessari seguir el següent procediment:

- El primer pas és activar l'opció `boot_wait`. Per a fer això s'ha de posar a "on" l'opció en el menú Administration, Management i a continuació guardar els canvis. Una altra forma de realitzar aquest pas mitjançant la línia de comandes és:

```
nvramp set boot_wait=on
nvramp commit
```

- Obrir una finestra de símbol del sistema i escriure, sense prémer enter, el següent:

```
tftp -i 192.168.1.1 PUT XXXX-X.X.X-XX.bin
```

- Obrir una altra finestra de símbol del sistema per a realitzar un ping continu cap al router:

```
ping -t 192 192.168.1.1
```

- A continuació endollar l'alimentació al router i, en el moment en què el ping retorni una contestació positiva, prémer enter en la finestra on està preparada la comanda ftp.
- A continuació cal esperar uns instants i el router quedarà flashejat.

A1.2. Configuració OLSR

OLSR utilitza un fitxer per a ser configurat. Per tant, per a modificar els valors dels paràmetres o bé per afegir extensions al protocol base s'ha de modificar aquest fitxer. Aquest fitxer està localitzat en la ruta:

```
/var/etc/olsrd.conf
```

El contingut d'aquest fitxer és el següent:

```
DebugLevel          0
IpVersion           4
AllowNoInt          yes
Pollrate            0.1
TcRedundancy        2
MprCoverage         7
LinkQualityFishEye  1
LinkQualityWinSize  100
LinkQualityDijkstraLimit 0 9.0
LoadPlugin "olsrd_dyn_gw_plain.so.0.4"
{
}
```



```
LoadPlugin "olsrd_nameservice.so.0.2"
{
    PlParam "name"          "AP3"
    PlParam "hosts-file"   "/var/etc/hosts"
    PlParam "suffix"       ".olsr"
}
LoadPlugin "olsrd_txtinfo.so.0.1"
{
    PlParam "Accept" "127.0.0.1"
}
Hna4
{
    0.0.0.0 0.0.0.0
}
IpcConnect
{
    MaxConnections 1
    Host           127.0.0.1
}
LinkQualityLevel 2
UseHysteresis no
Interface "vlan0"
{
    HelloInterval          6.0
    HelloValidityTime     108.0
    TcInterval             4.0
    TcValidityTime        324.0
    MidInterval            18.0
    MidValidityTime       324.0
    HnaInterval           18.0
    HnaValidityTime       108.0
}
# Add your addons (e.g. plugins) to olsrd.conf here,
# addons for interfaces in /etc/local.olsrd.conf.eth1
```

ANNEX 2: CONFIGURACIONS

A2.1. Introducció

L'objectiu d'aquest annex és recollir les configuracions comentades i el màxim d'informació sobre els escenaris provats.

Tota la informació aquí recollida ha de facilitar al màxim la reproductibilitat dels escenaris.

A2.2. Escenari 1

L'objectiu d'aquest escenari és estudiar el funcionament bàsic d'una xarxa mallada utilitzant el protocol OLSR. La xarxa de l'escenari està formada per 3 routers i l'objectiu és que el router 1 pugui accedir a Internet a través d'una porta d'accés situada a la xarxa. Per arribar a aquesta porta a Internet és necessari traçar una ruta a través d'un altre node. D'aquesta manera es pot apreciar la funcionalitat de routing del protocol.

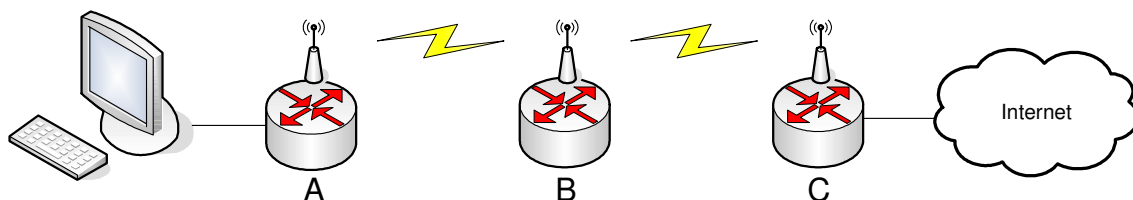


Fig. A2.1 Primer escenari amb OLSR

La configuració de tots els routers és la mateixa, a diferència del camp HNA4 del router que té la porta d'accés a Internet. La configuració dels nodes s'ha realitzat mitjançant l'aplicació web del firmware Freifunk utilitzat en aquests escenaris. A continuació es pot veure la configuració dels nodes:

Router 1:

```
Host Name: AP1
DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP adress: 10.10.1.1
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
```

```

ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP:
WAN Network Mask: 255.255.255.0
WAN GATEWAY:
HNA4:

```

Router 2:

```

Host Name: AP2
DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP address: 10.10.1.2
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP:
WAN Network Mask:
WAN GATEWAY:
HNA4:

```

Router 3:

```

Host Name: AP3
DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP address: 10.10.1.3
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP: 147.83.35.118
WAN Network Mask: 255.255.255.0
WAN GATEWAY: 147.83.35.2
HNA4: 0.0.0.0/4

```

Dins de l'anàlisi d'aquest escenari s'ha considerat important mostrar quins són els recursos consumits pel protocol. Per tant, a continuació es descriu la càrrega de CPU i el consum d'amplada de banda d'un dels nodes. S'han de tenir en compte els valors dels paràmetres del protocol utilitzats en realitzar aquest anàlisi i que el node compleixi el rol d'MPR.

```

HNA DESACTIVAT
POLL INTERVAL: 0,1
HELLO INTERVAL: 2
MID INTERVAL: 5
TCP INTERVAL: 5

```

Per a l'anàlisi del consum de CPU s'ha utilitzat l'eina top de Linux:

```

Mem: 8300K used, 6120K free, 0K shrd, 804K buff, 2820K cached
Load average: 0.09, 0.09, 0.06      (State: S=sleeping R=running,
W=waiting)

```

PID	USER	STATUS	RSS	PPID	%CPU	%MEM	COMMAND
974	root	S	560	697	0.7	3.8	dropbear
4677	root	R	360	2093	0.3	2.4	top

```

901 root      R          572      1  0.0  3.9  olsrd
2093 root      S          464     974  0.0  3.2  ash

```

En l'anàlisi de consum de CPU es pot observar un consum de CPU molt baix. El fet que hi hagi un nombre tan reduït de nodes fa que el consum de CPU es trobi en aquests valors.

En la imatge A2.1 es pot observar l'amplada de banda que consumeix el node B. Aquest gràfic ha estat filtrat per a que tan sols tingui en compte els paquets provinents d'aquest node.

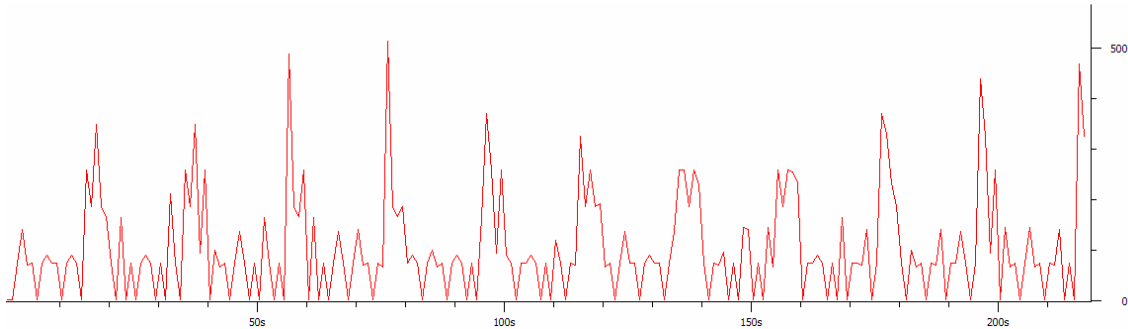


Fig. A2.2 Amplada de banda consumida en bytes/s per a un node

Pel que fa a l'anàlisi de consum d'amplada de banda, aquest depèn molt dels valors dels paràmetres utilitzats en la configuració del protocol. Els valors triats són uns valors recomanats per a xarxes petites. Per a xarxes més grans es recomana utilitzar valors més elevats per a reduir el consum de recursos. En el gràfic es pot apreciar un consum bastant disminuït d'amplada de banda. S'ha de tenir en compte, tanmateix, que aquest consum només pertany a un node. Per tant, per a xarxes amb més nodes, aquest valor és múltiple en relació a la quantitat de nodes en la xarxa.

A2.3. Escenari 2

El segon escenari pretén estudiar la possibilitat d'afegir mobilitat a la xarxa. Tal com està muntada ara la xarxa GUIFI.NET no permet mobilitat. En cas que un node es mogui dins les zones de cobertura de diferents nodes, l'usuari ha de canviar la connexió i la configuració per tal de connectar-se a un altre router.

La configuració de tots els routers és la mateixa a diferència del camp HNA4 del router que té la porta d'accés a Internet. La configuració dels nodes s'ha realitzat mitjançant l'aplicació web del firmware Freifunk utilitzat en aquests escenaris. A continuació es pot veure la configuració dels nodes:

Router 1:

```
Host Name: AP1
```

DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP adress: 10.10.1.1
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP:
WAN Network Mask: 255.255.255.0
WAN GATEWAY:
HNA4:

Router 2:

Host Name: AP2
DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP adress: 10.10.1.2
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP:
WAN Network Mask:
WAN GATEWAY:
HNA4:

Router 3:

Host Name: AP3
DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP adress: 10.10.1.3
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP: 147.83.35.118
WAN Network Mask: 255.255.255.0
WAN GATEWAY: 147.83.35.2
HNA4: 0.0.0.0/4

Ordinador portàtil:

Host Name: ABCD
DNS: 208.67.222.222;208.67.220.220
WLAN protocol: OLSR
WLAN IP adress: 10.10.1.10
WLAN Network Mask: 255.255.255.0
WLAN mode: Ad-hoc
ESSID: GUIFI
BSSID: 02:F4:37:80:8C:FC
WAN IP:
WAN Network Mask:
WAN GATEWAY:
HNA4:

A2.4. Escenari 3

La finalitat d'aquest escenari és l'aplicació de l'extensió de seguretat que inclou el protocol en el RFC.

Per afegir l'extensió de seguretat al protocol, en primer lloc s'ha d'instal·lar el paquet corresponent. Aquest paquet és l'anomenat "olsrd-mod-secure":

```
ipkg install olsrd-mod-secure
```

A continuació, s'ha de configurar-ne la inicialització en el fitxer de configuració `/var/etc/olsrd.conf`. Les línies de codi que s'han d'afegir en la secció d'extensions per a activar aquesta funció són les següents:

```
LoadPlugin "olsrd_secure.so.0.5"
{
    PlParam "keyfile" "/etc/olsrd.d/olsrd_secure_key"
}
```

En aquesta configuració s'indica l'arxiu "olsrd_secure_key" com a contenidor de la clau utilitzada per a crear la firma.

A2.5. Escenari 5

En aquest apartat es pretén estudiar les millores introduïdes per el algoritme B.A.T.M.A.N., un protocol creat per a arribar a ser un dia el substitut de l'OLSR.

Per a la configuració del escenari ja instal·lat el paquet Batmand:

```
ipkg update
ipkg install batmand
```

Anàlisi del consum de CPU del escenari amb B.A.T.M.A.N. utilitzant l'eina top de Linux:

```
Mem: 8268K used, 6152K free, 0K shrd, 792K buff, 3076K cached
Load average: 0.18, 0.09, 0.03      (State: S=sleeping R=running,
W=waiting)
```

PID	USER	STATUS	RSS	PPID	%CPU	%MEM	COMMAND
1758	root	S	568	852	0.5	3.9	dropbear
6702	root	R	360	1759	0.3	2.4	top
1759	root	S	464	1758	0.0	3.2	ash
852	root	S	380	1	0.0	2.6	dropbear
86	root	S	316	1	0.0	2.1	syslogd
85	root	S	280	1	0.0	1.9	klogd
6165	root	S	212	1	0.0	1.4	batmand
6166	root	S	212	6165	0.0	1.4	batmand
6167	root	S	212	6166	0.0	1.4	batmand

En l'anàlisi de consum de CPU es pot observar un consum de CPU molt baix molt semblant al que ja s'havia obtingut en el escenari d'OLSR. El fet que hi hagi un nombre tan reduït de nodes fa que el consum de CPU es trobi en aquests valors.

Per a la realització de les comparacions entre ambdós protocols es va utilitzar el mateix escenari amb la mateixa configuració. Aquest escenari és el següent:

- La configuració consisteix en un "Intel(R) Core(TM)2 CPU T7200 @ 2.00GHz" amb un sistema operatiu Linux de distribució gentoo 32-bits i utilitzant openVZ per a la virtualització de nodes
- La configuració de la xarxa consisteix en una topologia fixa sense pèrdua de paquets. Això es va aconseguir virtualitzant diverses instàncies de Linux i utilitzant ebtables per a permetre només els paquets entre nodes veïns.
- Una sola interfície de xarxa per a cada node.
- OLSR 0.5.0 es va utilitzar amb la implementació de olsrd amb els següents valors de configuració.
 - Hysteresis no
 - LinkQualityLevel 2, LinkQualityWinSize 100
 - Pollrate 0.05
 - NicChgsPollInt 3.0
 - RcRedundancy 2
 - MprCoverage 5
 - HelloInterval 5.0, HelloValidityTime 200
 - TcInterval 0.5, TcValidityTime 250.0
 - MidInterval 5.0, MidValidityTime 100.0
- B.A.T.M.A.N 0.2 es va utilitzar amb la implementació batmand amb els següents valors de configuració:
 - Originator interval: 5000
 - NBRF range: 10
 - TTL: 62

ANNEX 3: THE WIRELESS COMMONS MANIFESTO

We have formed the Wireless Commons because a global wireless network is within our grasp. We will work to define and achieve a wireless commons built using open spectrum, and able to connect people everywhere. We believe there is value to an independent and global network which is open to the public. We will break down commercial, technical, social and political barriers to the commons. The wireless commons bridges one of the few remaining gaps in universal communication without interference from middlemen and meddlers. Humanity is on the verge of a turning point because the Internet has transformed the way humans relate with one another. All communication can be traced to a human relationship, whether it's lovers exchanging instant messages or teenagers sharing music. The Internet has given us the ability to communicate faster and more cheaply than ever before in history.

The Internet's value increases exponentially with the number of people who are able to participate. In today's world, communication can take place without the use of antiquated telecommunications networks. The organizations that control these networks are limping anachronisms that are constrained by the expense and physical necessity of using wires to build their networks. Because of this, they cannot serve the great mass of people who stand to benefit from a wireless commons. Their interests diverge from ours, and their control over the network strangles our ability to communicate.

Low-cost wireless networking equipment which can operate in unlicensed bands of the spectrum has started another revolution. Suddenly, ordinary people have the means to create a network independent of any physical constraint except distance. Wireless can travel through walls, across property boundaries and through a community. Many communities have formed worldwide to help organize these networks. They are forming the basis for the removal of the traditional telecommunication networks as an intermediary in human communication.

The challenge facing community networks is the one limiting factor of wireless communication: distance. The relationships that can be formed across a community wireless network are limited by their physical reach. Typically these networks are growing to the size of a city, and growth beyond that point requires coordination and a strategic vision for community wireless networks as a whole. Without this coordination, it is hard to see how the worldwide community of wireless networking groups will ever merge their systems and create a true alternative to existing telecommunication networks.

There are many barriers to the creation of a global network. So far, the focus has been on identifying the technical barriers and developing methods to overcome them. But technical problems are the least of our worries, the business, political and social issues are the real challenges facing community networks. Hardware and software vendors need to understand the business rationale for implementing our technical solutions. Politicians need to understand our requirements for universal access to open spectrum. The public

needs to understand that the network exists and how to get access. Unless these problems are identified and addressed, the community wireless movement will never have influence beyond a local level.

Most importantly, the network needs to be accessible to all and provisioned by everyone who can provide. By adding enough providers to the network, we can bridge the physical gaps imposed by the range of our equipment. The network is a finite resource which is owned and used by the public, and as such it needs to be nurtured by the public. This, by its very nature, is a commons.

Becoming a part of the commons means being more than a consumer. By signing your name below, you become an active participant in a network that is far more than the sum of its users. You will strive to solve the social, political and technical challenges we face. You will provide the resources your community consumes by co-operating with total strangers to build the network that we all dream of.

ANNEX 4: LLICÈNCIA COMUNS SENSEFILS

1. Sobre el comuns sensefils **Comuns Sensefils**

1. El comuns sensefils descriu els termes i condicions per fer xarxa oberta per tal de que aquells individuals, col·lectius, empreses o administracions que ho desitgin i fan xarxa s'hi puguin acollir, o bé hi puguin manifestar el seu suport.
 1. Formulari d'adhesió d'una xarxa o signatura de suport al Comuns Sensefils
 2. Llistat de adhesions i signatures
 3. Enllaça la teva web amb el comuns sensefils
2. Quan la comunicació és sensefils, es refereix la utilització en exteriors de l'espai radioelèctric que no requereix de cap llicència.
3. Els principis generals de la declaració de llicència de comuns sensefils s'inspiren en fer xarxa lliure i oberta i es poden resumir en:
 1. Ets lliure d'utilitzar la xarxa per qualsevol propòsit en tant que no perjudiquis al funcionament de la pròpia xarxa o a la llibertat dels altres usuaris.
 2. Ets lliure de saber com és la xarxa, els seus components i com funciona.
 3. Ets lliure de fer ús de xarxa per a qualsevol tipus de comunicació i difondre'n el seu funcionament.
 4. Incorporant-te a la xarxa, ajudes a estendre aquestes llibertats en les mateixes condicions.

2. Sobre la xarxa oberta

1. La xarxa oberta és una expressió de valors fonamentals com la llibertat, la igualtat d'oportunitats i la solidaritat i fraternitat a través del dret a comunicar-se lliurement i a extreure'n el màxim de prestacions possibles. En cas de qualsevol dubte sobre algun aspecte concret, sempre ens referirem a aquests principis fonamentals.
2. La xarxa permet l'accés a tothom qui ho vulgui, i és el resultat de intercomunicar tots els seus membres amb la única condició de respectar el comuns sensefils. Si hi ha mecanismes de control en el seu accés es faran servir per a la correcta gestió de la xarxa des d'un punt de vista tecnològic i mai per a excloure l'accessibilitat.
3. Si bé els equips i infraestructures poden respondre a múltiples models de propietat o titularitat, la xarxa com a tal mai no pot tenir mai cap amo o propietari, amb independència de quina sigui l'aportació de cada part a la xarxa.
4. Els participants de la xarxa oberta que s'acullen al comuns sensefils, extenen la cobertura de la xarxa en les mateixes condicions del comuns sensefils, acceptant el lliure trànsit de comunicacions d'altres membres, sense manipular-lo més enllà del necessari per a la gestió de la xarxa.

5. Els membres de la xarxa oberta es comprometen únicament als termes i condicions del comuns sensefils. Qualsevol altre compromís l'han d'expressar explícitament.
6. Els membres de la xarxa, per tal de facilitar-ne el creixement i connectivitat, es comprometen a posar en consideració l'atorgament de permís per a deixar instal·lar equips propietat d'altres membres en les seves instal·lacions, tot i que sempre es reserven la darrera paraula en aquest sentit i encara que ho autoritzin, aquesta autorització no genera cap servitud i és revocable.
7. L'adhesió a la xarxa es pot expressar a títol individual o col·lectiu, i comporta l'acceptació dels termes del comuns sensefils. En qualsevol moment un membre adherit a la xarxa pot anul·lar la seva adhesió, recuperant la disposició dels equips dels que sigui propietari (apadrinat) de forma exclusiva, la titularitat o propietat no es perd mai independentment de on estiguin instal·lats.

3. Sobre la gestió de la xarxa i prioritats en el tràfic (qualitat de servei)

1. La gestió de la xarxa ha de ser pública i tothom qui ho desitgi ha de poder participar-hi.
2. Quan sigui possible, les prioritats del tràfic generals s'implementen en aquest ordre:
 1. Trànsit de tipus interactiu (missatgeria instantània, conferències de veu, navegar, etc.)
 2. Trànsit de tipus massiu o diferit (transferències, correu electrònic, còpies, etc.)
3. Els membres de la xarxa faran públiques les prioritats implementades en els seus trams de xarxa que puguin afectar als altres usuaris en cas de modificar les expressades en el punt anterior i que vagin més enllà de simplement donar-se prioritat en el seu tram de xarxa.
4. No es pot garantir la disponibilitat de la xarxa com a tal de forma global. Tanmateix la millor garantia és la transparència: En funció de les possibilitats, es procurarà publicar informació sobre la disponibilitat i estat de la xarxa. En trams concrets, qui vulgui pot oferir garanties de nivell de serveis si s'en fa càrrec, explica com ho fa i en quines condicions.

4. Sobre l'espai radioelèctric

1. Es considera l'ús en exteriors de l'espai radioelèctric que no requereix llicència com un bé d'ús universal, talment com l'aire o l'aigua, on l'ús obert com el descrit en el comuns sensefils o similars prevaleix davant de l'ús privatiu o explotació comercial. Es demana als governs, legisladors i organismes reguladors que crein els espais necessaris i facin les regulacions perquè això sigui possible.
2. Qui s'acull als comuns sensefils es compromet a fer-ne un ús responsable i a no excedir-se innecessàriament en les potències d'emissió.

5. Sobre la Seguretat

1. Cada membre de la xarxa és responsable de la seva seguretat, evitar intrusió en els seus propis sistemes d'informació i de xifrar les seves comunicacions si així ho desitja. La xarxa oberta simplement proporciona el mitjà de transport per fer-ho possible.

Es poden connectar xarxes privades a la xarxa oberta, i posar-hi tallafocs per controlar-ne l'accès. Aquests trams de xarxes queden exclosos del comuns sensefils i de la seva seguretat s'en fa càrrec qui la munta.

2. La xarxa oberta no es fa responsable de cap dany causat als seus membres durant l'ús de la xarxa.

6. Sobre la responsabilitat

1. La xarxa oberta mai és responsable de l'ús que en fan els seus membres.

7. Sobre els continguts.

El Comuns Sensefils descriu els termes i condicions per a fer xarxa oberta, però no inclou de cap manera ni els serveis que s'hi ofereixen, inclòs internet, ni els continguts. Per a les condicions dels seus continguts o els serveis que s'hi puguin oferir a través de la xarxa ja hi han múltiples formulacions de llicències. Tanmateix es recullen uns principis generals que són els següents:

1. Hi ha llibertat de crear continguts i serveis de qualsevol tipus per a tothom qui vulgui.
2. La xarxa oberta és el suport sobre el qual es fa la transmissió lliure dels continguts, però no hi té res a veure ni n'és responsable.
3. Els creadors o titulars dels continguts escullen el termes i condicions per al seu ús. Si no n'expressen, s'entén que son de lliure distribució en les mateixes condicions, tal i com es descriuen en el Creative Commons (by-sa). Quan es tracta de servidors que ofereixen alguna funcionalitat als usuaris, si no s'especifica el contrari o es diu que és "tal qual és" s'entén que es tracta d'una autoprestació col·lectiva sobre la que no s'ofereix cap tipus de garantia.
4. Els seus membres es comprometen a no fer trànsit per la xarxa de continguts inapropiats o ilegals, que puguin perjudicar a la resta de membres de la xarxa, ofensius, missatges no sol·licitats i similars continguts indesitjables.
5. Sobre l'accés a internet hi ha dos models:
 1. Basat en la explotació dels excedents d'accessos de membres de la xarxa. En aquest context, quan es fa sense contraprestació econòmica, l'accés a internet és un privilegi que et dona qui comparteix aquest excedent, no pas un dret ni tampoc un servei. La xarxa actúa com al vehicle que permet una consolidació agregada d'autopestacions, i com a tal, no hi apliquen les disposicions reguladores dels mercats

de telecomunicacions ni cap restricció contractual o regulació sobre la redistribució de l'ample de banda.

2. Accés a internet com a servei. En aquest model els usuaris d'aquest accés poden adoptar les fórmules de financiació i gestió que acordin oportunes.
6. La xarxa com a tal no pot donar garanties de disponibilitat de l'accés a internet o cap altre servei. Si algú en vol oferir o en vol gaudir ho pot fer de la manera que es descriu en l'apartat 3.4: Els adherits a la xarxa tenen llibertat per oferir-ne o contractar-ne dins de l'àmbit sobre qualsevol component de la xarxa.

8. El text d'aquesta declaració de Comuns Sensefils és sota aquesta llicència Creative Commons.

- No s'en pot fer un ús comercial
- La distribució i còpia és lliure referenciant que prové d'aquest Comuns Sensefils
- Es poden modificar els continguts i fer-ne treballs derivats si el resultat es distribueix de nou sota les mateixes condicions.