Treball Fi de Carrera

Desenvolupament d'una xarxa telemàtica per proveir accés a Internet al municipi de Molló

Antonio Casado Gutiérrez

Índex

Títol del projecte

Desenvolupament d'una xarxa telemàtica per proveir accés a Internet al municipi de Molló

Fases del projecte

El present projecte es desenvoluparà en tres fases:

- En aquesta primera fase, farem una petita descripció i objectius del projecte, a on inclourem un anàlisi del municipi i tota la informació relacionada amb els aspectes legals, sobre la instal·lació d'una xarxa sense fils en un ajuntament d'un petit municipi. També inclourem un estudi en detall dels estàndards de comunicació Wifi, Wimax, els tipus d'antenes i topologies de xarxa, per poder argumentar les característiques de cadascuna de les tecnologies, en aquesta fase també parlarem de la propagació de les radio freqüències i la relació de les ones estacionaries.
- En aquesta segona fase, parlarem dels equips escollits i farem ús de l'eina Radio Mobile per fer una simulació dels radioenllaços i la configuració dels mateixos.
- Per ultim a la tercera fase, veurem la viabilitat econòmica, les conclusions i un annex i bibliografia del projecte.

Objectius del projecte

L'objectiu del projecte es realitzar un anàlisi, disseny i implementació d'una infraestructura al municipi de Molló perquè l'Ajuntament pugui proporcionar al nucli del poble i dels veïnats de Molló, Internet a través d'un sistema sense fils. Per tal d'aconseguir aquests objectius, hauré de complir els següents punts, que passo a enumerar:

- Proveir d'una bona cobertura a tots els nuclis, tant del municipi de Molló, com els veïnats que ho conformen.

- Analitzar les possibles solucions i seleccionar la més adient perquè sigui una xarxa segura i escalable.

- Estimació econòmica de la infraestructura.

- Buscar possibles formes de finançament, per tal que sigui un projecte sostenible.

- Verificar el compliment de la normativa d'emissions en l'espectre radioelèctric.

Descripció del projecte

El projecte pretén analitzar les característiques geogràfiques bàsiques per tal de definir la infraestructura i equipament necessari que caldrà instal·lar al municipi de Molló per tal d'obtenir una xarxa de comunicacions que conformi un servei d'accés a Internet sense fils. Podrem oferir diferents modalitats de pagament en funció de les velocitats demandades, un rang gratuït de baixa velocitat per turistes i de pagament amb una franja de velocitats més alta per la resta de població que es donés d'alta al servei.

Amb el projecte es vol dotar de connexió a Internet a un total de 9 veïnats o entitats de població que conformen el municipi.

També es garantirà cobertura a emplaçaments on existeixi una concentració d'usuaris més alta com poden ser les entitats culturals i les zones verdes i l'església, com a centre del poble.

Molló és un municipi petit situat al nord-est de la comarca del Ripollès, amb una extensió de 43 Km² i està format per nou entitats de població, mes endavant farem un anàlisi del municipi amb molta mes profunditat. La població censada i que viu normalment en el poble no supera els 350 habitants, segons fonts del Institut Nacional d'Estadística. [(1)]

La població en caps de setmana i festius es veu triplicada, per tant la solució haurà d'estar dimensionada per a una quantitat d'usuaris superior a la censada, en el nostre cas per tal de garantir el servei a les demandes, ens basarem en 1050 habitants. Encara que pugin ser pocs habitants, degut a la dispersió geogràfica del municipi, si dotem d'aquests serveis a la població es podrien oferir avantatges, que enumeraré tot seguit:
Teletreball, Comerç online, Informació i serveis municipals, servei de publicitat per oferir allotjament, on menjar, com arribar, agenda d'activitats, entre d'altres.

Viabilitat (econòmica)

Per tal d'analitzar la viabilitat del projecte a la població de Molló, tindrem en consideració el numero d'habitants censats, mes el número de persones que de manera itinerant formen part de la població els caps de setmana i festius. Segons les dades del Institut Nacional d'Estadística, en el municipi de Molló hi ha un total de 350 habitants censats, aquesta xifra es veu triplicada en dies festius, per tant i seguint la normativa legal aplicable a aquest projecte, la velocitat no hauria de superar els 256 Kbps, sent aquesta conectivitat limitada a 30 minuts per usuari i dia.

Com que en una primera fase i degut a que es una solució escalable, no intentarem assolir més del 50% de la població total. Per tant, caldrà contractar al proveïdor de serveis d'internet ISP un servei de com a mínim 125Mbps.

També es proposa un suport de wifi de pagament per tal de tenir una velocitat superior fins a 6 Mbps i sense límit de temps. Les aportacions van dirigides íntegrament al manteniment de la infraestructura i a millorar l'accessibilitat TIC del municipi.

1 http://www.idescat.cat/emex/?id=171077

Les modalitats de quotes ofertades amb una velocitat de fins a 6 Mbps, són:

1 any: 42,00 € Soci anual
1 mes: 10,00 € Soci temporal
1 setmana: 6,00 € Soci col·laborador
1 dia (24h): 3,00 € Soci simpatitzant
15 minuts: 0,10 cents Soci passavolant

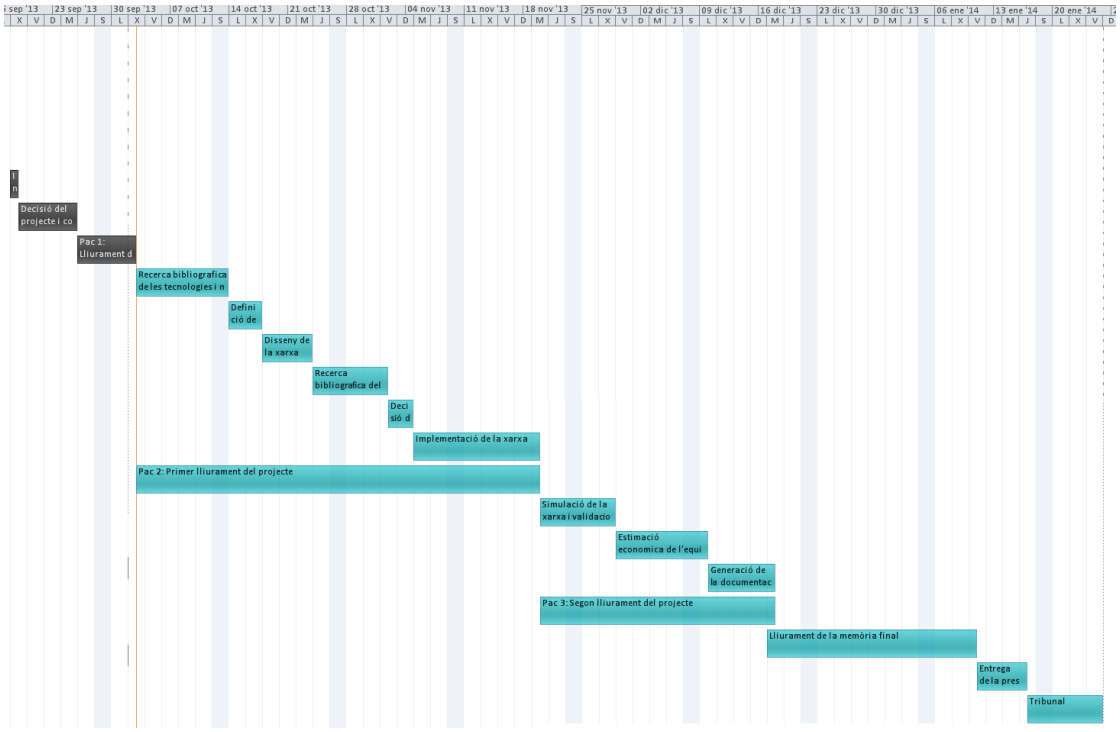
Per tal de veure si el projecte es viable, simularem que es fan socis nomes el 30% de la població censada en el municipi i que les quotes escollides son anuals, no tenint en compte altres modalitats de socis ofertades per aquesta simulació. De tal manera que tindrem 105 abonats, els quals pagarien una quota mensual de 42€ al mes, amb una permanència mínima de dos anys. Com que el pressupost del projecte és aproximadament de 74000€, durant el segon any i amb una previsió molt pessimista del retorn de la inversió tindríem el projecte amortitzat, per tant això fa que el projecte sigui viable en termes econòmics.

num.socis	quota	mesos	quantitat	
105	42 €	12	52.920 €	El primer any
105	42 €	12	52.920 €	segon any
			105.840 €	Total ingressos

Planificació del treball (diagrama de Gantt)

Inici del curs
Decisió del projecte
Lliurament del pla de treball
Recerca bibliogràfica de les tecnologies i normatives vigents
Definició de l'escenari
Disseny de la xarxa
Recerca bibliogràfica dels dispositius i infraestructures
Decisió de les màquines a instal·lar
Implementació de la xarxa
Primer lliurament del projecte
Simulació de la xarxa i validació del sistema
Estimació econòmica de l'equipament i de les tasques a realitzar
Generació de la documentació
Segon lliurament del projecte
Lliurament de la memòria final
Entrega de la presentació i del codi (si s'escau)
Tribunal

Modo de	Nombre de tarea	Duración	Comienzo	Fin
	Tribunal	7 días	vie 17/01/14	sáb 25/01/14
	Entrega de la presentació i del codi (si s'escau)	5 días	sáb 11/01/14	jue 16/01/14
	Lliurament de la memòria final	19 días	mar 17/12/13	vie 10/01/14
	Pac 3: Segon lliurament del projecte	20 días	mié 20/11/13	mar 17/12/13
	Generació de la documentació	6 días	mar 10/12/13	mar 17/12/13
	Estimació economica de l'equipament i de les tasques a realitzar	7 días	vie 29/11/13	lun 09/12/13
	Simulació de la xarxa i validacio del sistema	7 días	mié 20/11/13	jue 28/11/13
	Pac 2: Primer lliurament del projecte	34 días	jue 03/10/13	mar 19/11/13
	Implementació de la xarxa	11 días	mar 05/11/13	mar 19/11/13
	Decisió de les maquines a instal·lar	2 días	sáb 02/11/13	lun 04/11/13
	Recerca bibliografica dels dispositius i intraestructures	7 días	jue 24/10/13	vie 01/11/13
	Disseny de la xarxa	4 días	vie 18/10/13	mié 23/10/13
	Definició de l'escenari	4 días	lun 14/10/13	jue 17/10/13
	Recerca bibliografica de les tecnologies i normatives vigents	8 días	jue 03/10/13	dom 13/10/13
	Pac 1: Lliurament del pla de treball	5 días	jue 26/09/13	mié 02/10/13
	Decisió del projecte i comunicació al consultor	5 días	jue 19/09/13	mié 25/09/13
	Inici del curs	1 día	mié 18/09/13	mié 18/09/13

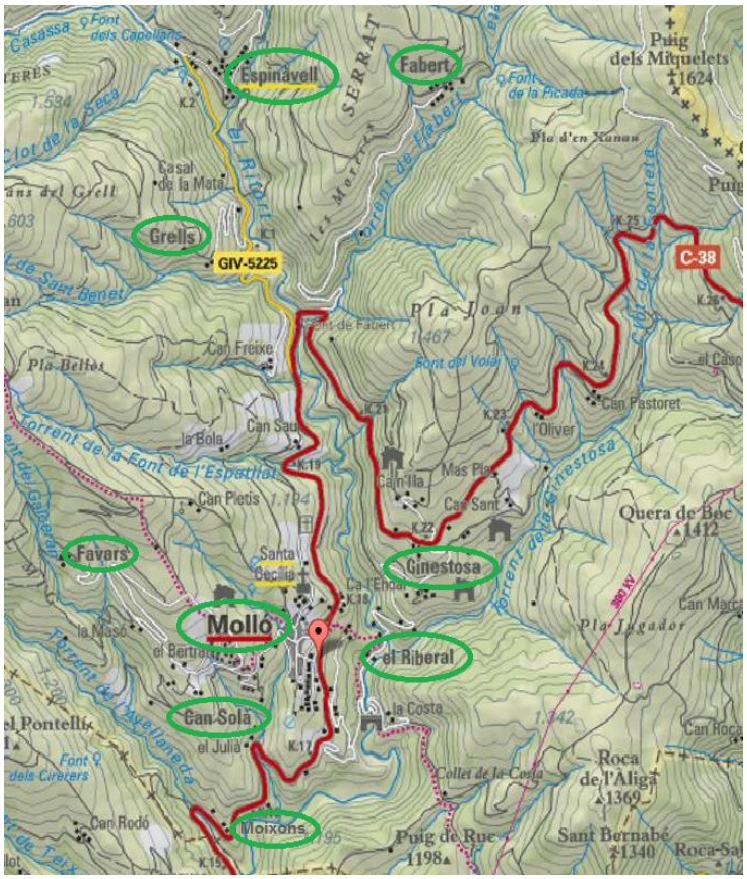


Anàlisi del municipi

Dedicarem una menció específica a l'estudi en profunditat del municipi degut al seu relleu muntanyós, penso que és important de cara a l'estudi de la cobertura entre veïnats.

Molló és un municipi situat al nord-est de la comarca del Ripollès, a la demarcació de Girona. Per la seva configuració física, el municipi forma part de l'anomenada Vall de Camprodon, a la capçalera del riu Ritort, afluent del Ter. El terme limita al nord amb el municipi de Prats de Molló i la Presta (Vallespir, França), a l'est i al sud amb el municipi de Camprodon, i a ponent amb els termes de Llanars i Setcases. El municipi té una extensió de 43 Km² i està format per nou entitats de població.

Detall de les diferents entitats amb el nombre d'habitants censats:
Can solà (14), Espinavell (42), Favars (33), Fabert (3), Ginestosa (23), Grells (7), Molló (206), Moixons (16), El Riberal(14).



Alguns llocs d'interès, representats a la imatge del mapa anterior, que cal destacar per tal de fer un estudi de cobertura suficient, serien:

Entitats culturals i pistes d'esports municipals, Ajuntament, zona que envolta l'Església.

Aspectes legals

Degut a que el nostre projecte consisteix en la implantació d'accés sense fils a Internet en espais públics i des de l'ajuntament, haurem notificar a la Comissió del Mercat de Telecomunicacions (CMT) de la nostra activitat per tal de tenir els aspectes legals ben coberts. Com que és de caràcter obligatori registrar-se, quan una administració pública vol donar servei d'accés a Internet a través de xarxes wifi, hem de complir una sèrie de condicions especials recollides a la llei General de Comunicacions 32/2003:

- Inscriuren's com operador en el registre d'operadors CMT [(2)]
- Separació comptable, per tal d'evitar transferència de fons públics.
- Operar d'acord als principis de neutralitat, transparència i no discriminació

2 http://www.cmt.es/

Llei General de les telecomunicacions

Un cop revisada la Llei publicada al BOE-264, de 4-11-2003, Llei 32/2003, de 3 de novembre, general de telecomunicacions podríem destacar una sèrie d'articles pertinents al nostre projecte i amb el rerefons de les administracions públiques, en el nostre cas, l'Ajuntament de Molló:

TÍTOL I

- ***Article 2. Les telecomunicacions com a serveis d'interès general.***

1. Les telecomunicacions són serveis d'interès general que es presten en règim de lliure competència.
2. Només tenen la consideració de servei públic o estan sotmesos a obligacions de servei públic els serveis que regulen l'article 4 i el títol III d'aquesta Llei. La imposició d'obligacions de servei públic persegueix la consecució dels objectius que estableix l'article 3 d'aquesta Llei i pot recaure sobre els operadors que obtinguin drets d'ocupació del domini públic o de la propietat privada, de drets d'ús del domini públic radioelèctric, o que tinguin la condició d'operador amb poder significatiu en un determinat mercat de referència."

- ***Article 3. Objectius i principis de la Llei.***

Els objectius i principis d'aquesta Llei són els següents:
a) Fomentar la competència efectiva als mercats de telecomunicacions i, en particular, l'explotació de les xarxes i la prestació dels serveis de comunicacions electròniques i el subministrament dels recursos que hi estan associats. Tot això promovent una inversió eficient en matèria d'infraestructures i fomentant la innovació.
b) Garantir el compliment d'aquestes condicions i de les obligacions de servei públic en l'explotació de xarxes i la prestació de serveis de comunicacions electròniques, en especial les de servei universal.
c) Promoure el desenvolupament del sector de les telecomunicacions, així com la utilització dels nous serveis i el desplegament de xarxes, i l'accés a aquestes, en condicions d'igualtat, i impulsar la cohesió territorial, econòmica i social.
d) Fer possible l'ús eficaç dels recursos limitats de telecomunicacions, com la numeració i l'espectre radioelèctric, i l'adequada protecció d'aquest últim, i l'accés als drets d'ocupació de la propietat pública i privada.

TÍTOL II - Explotació de xarxes i prestació de serveis de comunicacions electròniques en règim de lliure competència.
CAPÍTOL I

- ***Article 5. Principis aplicables.***

1. L'explotació de les xarxes i la prestació dels serveis de comunicacions electròniques s'ha de fer en règim de lliure competència sense més limitacions que les que estableix aquesta Llei i la seva normativa de desplegament.
2. L'adquisició dels drets d'ús de domini públic radioelèctric, d'ocupació del domini públic o de la propietat privada i dels recursos de numeració necessaris per a l'explotació de xarxes i per a la prestació de serveis de comunicacions electròniques s'ha de fer de conformitat amb el que disposa la seva normativa específica."

- ***Article 6. Requisits exigibles per a l'explotació de les xarxes i la prestació dels serveis de comunicacions electròniques.***

2. Els interessats en l'explotació d'una determinada xarxa o en la prestació d'un determinat servei de comunicacions electròniques, abans de l'inici de l'activitat, han de notificar-ho fefaentment a la Comissió del Mercat de les Telecomunicacions en els termes que es determinin

mitjançant un reial decret, i s'han de sotmetre a les condicions previstes per a l'exercici de l'activitat que pretenguin fer. Queden exempts d'aquesta obligació els qui explotin xarxes i prestin serveis de comunicacions electròniques en règim d'auto prestació."

- ***Article 8. Condicions per a la prestació de serveis o l'explotació de xarxes de comunicacions electròniques.***

1. L'explotació de les xarxes i la prestació dels serveis de comunicacions electròniques s'han de subjectar a les condicions que preveuen aquesta Llei i la seva normativa de desplegament, entre les quals s'hi ha d'incloure les de salvaguarda dels drets dels usuaris finals.
3. Les entitats públiques o privades que, d'acord amb la legislació vigent, tinguin drets especials o exclusius per a la prestació de serveis en un altre sector econòmic i que explotin xarxes públiques o prestin serveis de comunicacions electròniques disponibles al públic han de portar comptes separats i auditats per a les seves activitats de comunicacions electròniques, o establir una separació estructural per a les activitats associades amb l'explotació de xarxes o la prestació de serveis de comunicacions electròniques.

CAPÍTOL III
Secret de les comunicacions i protecció de les dades personals i drets i obligacions de caràcter públic vinculats amb les xarxes i serveis de comunicacions electròniques

- ***Article 33. Secret de les comunicacions.***

Els operadors que explotin xarxes públiques de comunicacions electròniques o que prestin serveis de comunicacions electròniques disponibles al públic han de garantir el secret de les comunicacions de conformitat amb els articles 18.3 i 55.2 de la Constitució, i han d'adoptar les mesures tècniques necessàries.

- ***Article 34. Protecció de les dades de caràcter personal.***

Sense perjudici del que preveuen l'apartat 6 de l'article 4 i el segon paràgraf de l'article anterior, així com la restant normativa específica aplicable, els operadors que explotin xarxes públiques de comunicacions electròniques o que prestin serveis de comunicacions electròniques disponibles al públic han de garantir, en l'exercici de la seva activitat, la protecció de les dades de caràcter personal de conformitat amb la legislació vigent. Els operadors als quals es refereix el paràgraf anterior han d'adoptar les mesures tècniques i de gestió adequades per preservar la seguretat en l'explotació de la seva xarxa o en la prestació dels seus serveis, a fi de garantir els nivells de protecció de les dades de caràcter personal que exigeixi la normativa de desplegament d'aquesta Llei en aquesta matèria. En cas que hi hagi un risc particular de violació de la seguretat de la xarxa pública de comunicacions electròniques, l'operador que exploti l'esmentada xarxa o presti el servei de comunicacions electròniques ha d'informar els abonats sobre l'esmentat risc i sobre les mesures que s'han d'adoptar."

- ***Article 36. Xifratge en les xarxes i serveis de comunicacions electròniques.***

1. Qualsevol tipus d'informació que es transmeti per xarxes de comunicacions electròniques pot ser protegida mitjançant procediments de xifratge.

TÍTOL V
Domini públic radioelèctric

- ***Article 43. Gestió del domini públic radioelèctric.***

1. L'espectre radioelèctric és un bé de domini públic, la titularitat, gestió, planificació, administració i control del qual corresponen a l'Estat. Aquesta gestió s'exerceix de conformitat amb el que disposen aquest títol i els tractats i acords internacionals en els quals Espanya és part, atenent la normativa aplicable de la Unió Europea i les resolucions i recomanacions de la Unió Internacional de Telecomunicacions i d'altres organismes internacionals.

TÍTOL VII

Taxes en matèria de telecomunicacions

- ***Article 49. Principis aplicables a les taxes en matèria de telecomunicacions.***

1. Els operadors i els titulars de drets d'ús del domini públic radioelèctric o de recursos de numeració han d'estar subjectes al pagament de les taxes que estableix l'ordenament jurídic.

2. Aquestes taxes tenen com a finalitat:

a) Cobrir les despeses administratives que ocasioni el treball de regulació relatiu a la preparació i posada en pràctica del dret comunitari derivat i actes administratius, com les relatives a la interconnexió i accés.

b) Els que ocasionin la gestió, el control i l'execució del règim que estableix aquesta Llei.

c) Els que ocasionin la gestió, el control i l'execució dels drets d'ocupació del domini públic, els drets d'ús del domini públic radioelèctric i la numeració.

d) La gestió de les notificacions que regulen l'article 6 d'aquesta Llei.

e) Les despeses de cooperació internacional, harmonització i normalització i l'anàlisi de mercat.

TÍTOL VIII - Inspecció i règim sancionador

- ***Article 50. Funcions inspectores i sancionadores.***

1. La funció inspectora en matèria de telecomunicacions correspon a:

a) L'Agència Estatal de Radiocomunicacions.

b) La Comissió del Mercat de les Telecomunicacions.

c) El Ministeri de Ciència i Tecnologia.

2. És competència del Ministeri de Ciència i Tecnologia la inspecció dels serveis i de les xarxes de telecomunicacions, de les seves condicions de prestació, dels equips, dels aparells, de les instal·lacions i dels sistemes civils, que compta amb un servei central d'inspecció tècnica de telecomunicacions.

3. Correspon a la Comissió del Mercat de les Telecomunicacions la inspecció de les activitats dels operadors de telecomunicacions respecte de les quals tingui competència sancionadora de conformitat amb aquesta Llei.

4. Correspon a l'Agència Estatal de Radiocomunicacions la competència de control i inspecció del domini públic radioelèctric, així com la realització d'activitats d'inspecció de conformitat amb el que estableix l'apartat següent.

- ***Article 52. Classificació de les infraccions.***

"Les infraccions de les normes reguladores de les telecomunicacions es classifiquen com a molt greus, greus i lleus."

Estàndard de la tecnologia WIFI

L'especificació IEEE 802.11 (ISO/IEC 8802-11) és un estàndard internacional que defineix les característiques d'una xarxa d'àrea local sense fils (WLAN). **Wifi** (que significa "Fidelitat inhalàmbrica", moltes vegades incorrectament abreviat Wifi) és el nom de la certificació atorgada por la Wifi Alliance, anteriorment WECA (Wireless Ethernet Compatibility Alliance), grup que garanteix la compatibilitat entre dispositius que utilitzen l'estàndard 802.11. Per a l'ús indegut dels termes (i per raons de màrqueting) el nom de l'estàndard es confon amb el nom de la certificació. Una xarxa Wifi és en realitat una xarxa que compleix amb l'estàndard 802.11. Als dispositius certificats per la Wifi Alliance es permet utilitzar aquest logotip:

Amb Wifi es poden crear xarxes d'àrea local sense fils d'alta velocitat sempre que l'equip que es vagi a connectar no estigui molt allunyat del punt d'accés. A la pràctica, Wifi admet ordinadors, portàtils, equips d'escriptori, assistents digitals personals (PDA), smartphones o qualsevol altre tipus de dispositiu d'alta velocitat amb propietats de connexió també d'alta velocitat (11 Mbps o superior) dintre d'un radi de vàries dotzenes de metres en ambients tancats (de 20 a 50 metros en general) o dintre d'un radi de cents de metres a l'aire lliure.

Els proveïdors de Wifi estan començant a cobrir zones amb una gran concentració d'usuaris (com estacions de trens, aeroports i hotels) amb xarxes sense fils. Aquestes zones es denominen "**zones locals de cobertura**".

L'estàndard 802.11 estableix els nivells inferiors del model OSI per a les connexions sense fils que utilitzen ones electromagnètiques, per exemple:

- La capa física (a vegades abreujada capa "PHY") ofereix tres tipus de codificació de informació.
- La capa d'enllaç de dades composta per dos subcapes: **control d'enllaç lògic**(**LLC**) i **control d'accés al medi** (**MAC**).

La capa física defineix la modulació de les ones de radio i les característiques de senyalització per a la transmissió de dades mentre que la capa d'enllaç de dades defineix l'interfaç entre el bus de l'equip i la capa física, en particular un mètode d'accés paregut al utilitzat a l'estàndard Ethernet, i les regles per a la comunicació entre les estacions de la xarxa. En realitat, l'estàndard 802.11 té tres capes físiques que estableixen modes de transmissió alternatius:

<table>
<tr><td rowspan="2">Capa d'enllaç de dades (MAC)</td><td>802.2</td></tr>
<tr><td>802.11</td></tr>
<tr><td>Capa física (PHY)</td><td><table><tr><td>DSSS</td><td>FHSS</td><td>Infraroig</td></tr></table></td></tr>
</table>

Qualsevol protocol de nivell superior pot utilitzar-se en una xarxa sense fils Wifi de la mateixa manera que pot utilitzar-se en una xarxa Ethernet.

Estàndards 802.11a, 802.11b, 802.11g i 802.11n

Els estàndards 802.11a, 802.11b, 802.11g i 802.11n, anomenats "estàndards físics", son modificacions de l'estàndard 802.11 i treballen de modes diferents, el que els permet arribar a diferents velocitats en la transferència de dades segons els seus rangs.

Estàndard	Freqüència	Velocitat	Rang
wifi a (802.11a)	5 GHz	54 Mbit/s	10 m
wifi b (802.11b)	2,4 GHz	11 Mbit/s	100 m
wifi g (802.11g)	2,4 GHz	54 Mbit/s	100 m
wifi n (802.11n)	2,4 GHz	300 Mbit/s	100 m

802.11a

L'estàndard 802.11a te en teoria un flux de dades màxim de 54 Mbps, cinc vegades el del 802.11b i nomes un rang de trenta metres aproximadament. L'estàndard 802.11a es basa en la tecnologia anomenada OFDM (*multiplexació per divisió de freqüències ortogonals*). Transmet en un rang de freqüència de 5 GHz i utilitza 8 canals no superposats.
És per aquest motiu que els dispositius 802.11a son incompatibles amb els dispositius 802.11b. Però, existeixen dispositius que incorporen tots dos xips el 802.11a i el 802.11b i s'anomenen dispositius de "**banda dual**".

Velocitat hipotètica	**Rang**
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

802.11b

L'estàndard 802.11b permet un màxim de transferència de dades de 11 Mbps en un rang de 100 metres aproximadament en ambients tancats i de més de 200 metres a l'aire lliure (o inclús més que això amb l'ús d'antenes direccionals).

Velocitat hipotètica	**Rang (en ambients tancats)**	**Rang (a l'aire lliure)**
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

802.11g

L'estàndard 802.11g permet un màxim de transferència de dades de 54 Mbps en rangs comparables als del estàndard 802.11b. A mes, i degut a que l'estàndard 802.11g utilitza el rang de freqüència de 2.4 GHz amb codificació OFDM, és compatible amb els dispositius 802.11b amb excepció d'alguns dispositius més antics.

Velocitat hipotètica	**Rang (en ambients tancats)**	**Rang (al aire lliure)**
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

802.11n

L'estàndard 802.11n permet un màxim de transferència de dades de 300 Mbps en rangs comparables als del estàndard 802.11g. S'obliga a tenir dispersió espacial , utilitzant tecnologia MIMO , la qual cosa, juntament amb la resta de característiques d'aquesta norma, permet un major abast que en les anteriors.

La norma 802.11n ofereix la possibilitat de funcionar en ambdues bandes , tant en 2,4 GHz com en 5 GHz Una de les grans avantatges de la nova norma és la compatibilitat amb les normes anteriors la qual cosa possibilita la integració de sistemes nous en xarxes ja existents i una migració senzilla i econòmica.

Per aconseguir aquesta major velocitat , els equips 802.11n segueixen dues estratègies : un major ample de banda del canal i ús de la tecnologia MIMO amb divisió per multiplexació espacial (SDM).

L'altra estratègia que segueix la norma 802.11n per aconseguir major velocitat és l'ús de tecnologia MIMO amb dispersió per separació espacial (SDM). Els equips 802.11n disposen sempre de diverses antenes per transmetre i altres tantes per rebre. El sistemes són capaços d'emetre un flux de dades diferent per cada antena, permetent així una major velocitat de global transmissió. Aquesta tecnologia necessita circuiteria específica per cada antena, en concret un emissor de ràdio i un conversió analògic/digital independent, la qual cosa redunda en un major cost i complexitat tècnica. Aquesta és la raó que existeixin diverses configuracions d'antenes, depenent de l'equip seleccionat.

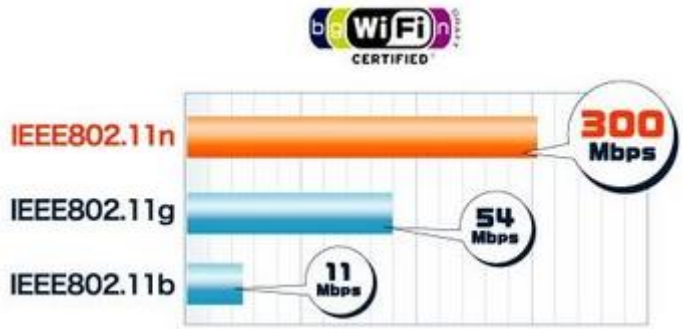
Aquesta configuració els permet tenir una major diversitat espacial , no per assolir una major velocitat de comunicació, sinó per obtenir una millor resistència davant interferències i proporcionar major abast.

Amb l'objecte d'incrementar la velocitat de transmissió , els sistemes 802.11n inclouen un concepte nou, no existent en les anteriors normes : la supertrama. Els equips 802.11n no transmeten la informació tal qual se'ls requereix , sinó que la encapsulen en una trama major per tal d'optimitzar la utilització de la ràdio. Aquesta característica, tot i ser teòricament desitjable, presenta diversos problemes en els equips, ja que han d'emmagatzemar la informació que els arriba per ser transmesa fins que conformen la supertrama. Així mateix han d'encaixar els paquets d'informació de manera eficient en la supertrama i en la recepció, han desempaquetar. Això suposa una major demanda dels equips 802.11ni una major potència de procés de la necessària en generacions anteriors, i és, així mateix, font de problemes en algunes implementacions, i no és estrany observar grans diferències en la velocitat de transmissió depenent del tipus de informació transmesa, sobretot per a certs mides de paquets o barreja de mides, a causa del procés d'empaquetat i desempaquetat i els algoritmes d'optimització d'aquest procés .

- MIMO:

Fins a 2004 les interfícies wifi tenien una única antena. fins i tot en configuracions dotades de diversitat, això significava que de dues o més antenes es prenia la qual rebés millor senyal, però la cadena d'entrada i la cadena de sortida eren úniques en el transceptor. El següent pas és dotar cada antena del seu pròpia cadena RF, de manera que cada antena pugui transmetre i rebre alhora que les altres. Això pot augmentar el throughput significativament, però a més permet obtenir beneficis afegits de processar les senyals rebudes simultàniament a l'hora d'enfrontar a la interferència per multi trajecte.

Comparativa entre diferents estàndards IEEE 802.11



La nostra freqüència de treball serà de 2.4 GHz, per aquest motiu nomes optarem pels estàndards 802.11 b/g/n, permetent una convivència amplia de normes, però experimentant una reducció significativa de velocitat en barrejar-ne de diferents en una mateixa xarxa.

Estàndard de la tecnologia Wimax

L'estàndard 802.16

L'estàndard 802.16 també anomenat Wimax sigles de Worldwide Interoperability for Microwave Access (interoperabilitat mundial per a accés per microones), es una norma de transmissió de dades que utilitza les ones de radio a les freqüències de 2,3 a 3,5 GHz i pot tenir un abast de fins 60 km.

Aquest estàndard també és conegut com a tecnologia d'última milla, per què una de les seves avantatges és donar serveis de banda ample a zones a on el desplegament de cable o fibra per la baixa densitat de població presenta uns costos per usuari molt elevats (zones rurals).

L'únic organisme habilitat per a certificar el compliment de l'estàndard i la interoperabilitat entre equipament de distints fabricants es el Wimax Forum: tot equipament que no tingui aquesta certificació, no pot garantir la seva interoperabilitat amb altres productes.

Actualment es recullen dintre de l'estàndard 802.16 dos variants:

- Un d'**accés fixe** (802.16d), en el que s'estableix un enllaç radio entre la estació base i un equip d'usuari situat en el domicili de l'usuari.

  Per a l'entorn fixe, les velocitats teòriques màximes que es poden obtenir son de 70 Mbit/s amb un ample de banda de 20 MHz. En entorns reals s'han aconseguit velocitats 20 Mbit/s amb ràdios de cèl·lula de 6 km, ample de banda que es compartit per tots els usuaris de la cèl·lula

- Un de **mobilitat complerta** (802.16e), que permet el desplaçament de l'usuari d'un mode similar al que es pot donar en GSM/UMTS, el mòbil, encara no es troba desenvolupat i actualment competeix amb les tecnologies LTE (basades en femtocelul·les, connectades mitjançant cable), per ser la alternativa per a les operadores que aposten pels serveis de mobilitat, aquest estàndard, en la seva variant "no llicenciada", competeix amb el Wifi IEEE 802.11n, ja que la majoria dels portàtils i dispositius mòbils, comencen a estar dotats d'aquest tipus de connectivitat.

Taula.- Evolució estàndard 802.16.

Standard	Velocitat hipotètica	Rang (a l'aire lliure)
802.16	32 a 134 Mbit/s (28Mhz)	1.6 a 4.83 Km
802.16a/REVd	Fins a 75 Mbit/s (20Mhz)	4.83 a 8.05 Km
802.16e	Fins a 15 Mbit/s(5Mhz)	1.6 a 4.83 Km

No obstant, existeixen una sèrie de grans diferencies entre ambdós sistemes, que fan que Wimax es converteixi en una plataforma mes eficaç i adequada que Wifi.

És important destacar que Wimax és un sistema de llarg abast, el qual permet cobrir una gran quantitat de kilòmetres, ja que utilitza l'espectre tant lliure com propietari, es a dir, amb llicencia o sense, per a oferir connexió a una xarxa, en la majoria dels casos d'Internet. Pel contrari, Wifi utilitza nomes l'espectre sense llicencia amb el fi de facilitar l'accés a una xarxa local, el que fa que el seu abast sigui mes limitat.

Encara que Wimax presenti mes avantatges, es cert que fins el moment Wifi continua sent més popular en dispositius d'usuari final. Una de las grans diferencies que existeixen entre les dos plataformes resideix en el fet que Wifi s'executa a través del protocol Media Access Control CSMA/CA, mentre que Wimax s'executa a traves d'una connexió orientada a MAC.

Wimax i Wifi tenen mecanismes de serveis molt diferents, ja que per una banda Wimax utilitza un mecanisme de QoS basat en les connexions que s'estableixen entre les estacions base i el dispositiu de l'usuari, cadascuna de les connexions establertes es basen en algoritmes de programació específiques. Per altre banda, Wifi utilitza afirmació d'accés i això pot arribar a interrompre la connexió d'acord al rendiment que ofereixi la xarxa utilitzada.

És important destacar que encara que Wifi i Wimax son tecnologies que han estat dissenyades per a ser aplicades en situacions diferents, certament es poden utilitzar de forma complementaria**.**

En l'actualitat la majoria dels operadors ofereixen el servei de xarxa Wimax, oferint a més a més,un segment especial que ofereix la possibilitat de connectar-se a la xarxa metropolitana de Wimax, al mateix temps que permet utilitzar la plataforma Wifi dintre de casa o la oficina, amb els dispositius locals que s'utilitzen per a connectar-se a internet, com es el cas de smartphones, tabletes, ordinadors, portàtils, entre d'altres. D'aquesta manera, a traves d'un simple selector d'unitat, l'usuari pot col·locar el receptor Wimax a l'àrea física a la que es rebi millor connectivitat, com pot ser per exemple una finestra, sent capaç de poder utilitzar la xarxa Wimax des de qualsevol lloc que es trobi dintre del perímetre en que es troba establerta la xarxa.

En l'estàndard IEEE802.16 (versió 2009) es defineixen quatre diferents especificacions per a la capa física PHY que poden usar en conjunt amb la capa MAC per donar una connexió extrem a extrem fiable.

Aquestes especificacions són les següents:

- WirelessMAN-SC, es tracta de la versió "Single Carrier" realitzada per a casos amb línia de vista directa (ELS) a la banda de freqüències de 10-66 GHz Aquesta versió aquesta enfocada per a aplicacions amb flexibilitat de configuració, ja que les antenes transmissora i receptora han de tenir vista directa entre elles, sent aquesta una raó per la qual l'antena receptora ha de situar en llocs alts.

- WirelessMAN-OFDM-256 FFT, projectada per a operacions sense línia de vista directa (NLOS) en bandes de freqüències inferiors a 11 GHz (2- 11GHz). Utilitza com a base la modulació ortogonal (OFDM). Aquesta versió suporta subcanalizacio a l'enllaç uplink (UL), que representa una gran eina per a la optimització en la cobertura del sistema.

- WirelessMAN-OFDMA-2048 FFT: Suporta operacions NLOS en bandes de freqüències inferiors a 11 GHz (2- 11GHz), i es basa en l'esquema de múltiple accés denominat OFDMA (Ortogonal Frequency Division Multiple Access). Es tracta d'una extensió de la tècnica OFDM per permetre el compartiment de la cadena per múltiples usuaris. A més, suporta subcanalització en ambdós enllaços, uplink (UL) i downlink (DL).

- WirelessHUMAN: Comprèn funcionalitats especifiques per funcionar en bandes sense llicència, sent per això anomenada "High Speed Unlicensed Metropolitan Area Network - HUMAN" Especifica l'operació en les bandes 5 a 6 GHz, utilitzant com a base un esquema flexible de canalització que inclou canals de 10 i 20 MHz, amb separacions de 5 MHz.

Tecnologies de Transmissió

OFDM (Ortogonal Frecuency Division Multiplexing)

La tecnologia OFDM (multiplexació per Divisio Ortogonal de freqüència), és en la qual es basa la interfície física Wireless MAN - OFDM, que esta dissenyada per enllaços NLOS. Aquesta tecnologia compta amb una quantitat de 256 subportadores, per bandes de freqüència per sota 11Ghz.

OFDM es basa en el principi d'ortogonalitat de freqüències adjacents en el qual cadascuna d'elles és modulada per un tren de dades de baixa velocitat. Consisteix en 256 portadores, dins de les quals 8 són utilitzades com a pilots (-84 , -60 , -36 , -12 , 12, 36 , 60 , 84) i 56 portadores són usades com guardes, per tant només ens queda 192 portadores per al transport de dades.

L'energia del transmissor s'incrementa amb la longitud del temps de guarda, mentre l'energia del receptor continua sense variació. La codificació del canal és definida en 3 passos:

- Randomization: es dóna en cada ràfega d'informació, ja sigui downlink o uplink.
- Codificació FEC: consisteix en una concatenació d'un codi Reed-Salomon de sortida i un codi intern de velocitat de connexió i interpolació compatibles.
- Interleaving: assegura que els bits adjacents codificats siguin mapejats en subportadores no adjacents. Així mateix evita la presència de bits de poca fiabilitat, això ho realitza mapejant una quantitat significativa de bits de constel·lació.

OFDMA (Ortogonal Frecuency Division Mutiple Access)

La tecnologia OFDMA (Acces Multiple per Divisió de Freqüència Ortogonal), tècnica base del tipus d'interfície físic Wireless MAN- OFDMA PHY, aquesta dissenyada per a l'operació NLOS per bandes de freqüències sota d'11 Ghz. En el cas que es tractés d'una banda llicenciada, l'ample de banda permès deu limitar-se per l'ample de banda provisional regulador dividit entre qualsevol potència de 2 no menor d'1 MHz. D'aquesta manera són suportats els tamanys 2048, 1024, 512 i 128 de FFT, el que facilita el suport de diversos amples de canal [IEEE1609].

Les subportadores actives són dividides en subconjunts de portadores on cadascuna d'aquestes serà assignada a un canal diferent. Així mateix les portadores que formen una cadena no necessàriament han de ser adjacents.

Pel que fa al domini del temps, l'estructura és la mateixa que al OFDM. Així mateix el domini de freqüències i la codificació de canal tenen les mateixes consideracions que a la tècnica anterior, OFDM.

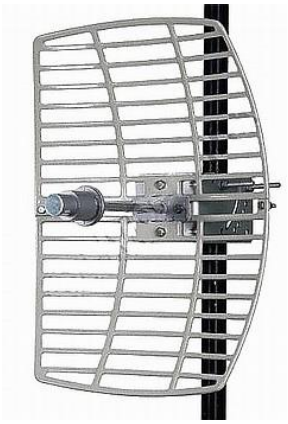
Algunes de les tècniques per a compensar els efectes causats per la propagació multitrajecte es presenten a continuació:

- AAS (Adaptive Antenna Systems) per adaptar el diagrama de radiació a una direcció o adreces privades.
- STC (Space Time Coding). Mecanismes que realitzen diversitat de transmissió.
- ARQ (Automatic RepeatreQuest): Protocols utilitzats per al control de errors que retransmet els paquets que no van arribar correctament al seu destí.

Tipus d’antenes

Antenes Direccionals

Aquestes orienten el senyal en una direcció molt determinada amb un feix estret però de llarg abast, actua de forma semblant a un focus de llum que emet un feix concret i estret però de forma intensa (més abast).
L'abast d'una antena direccional ve determinat per una combinació dels dBi de guany de l'antena, la potència d'emissió del punt d'accés emissor i la sensibilitat de recepció del punt d'accés receptor.

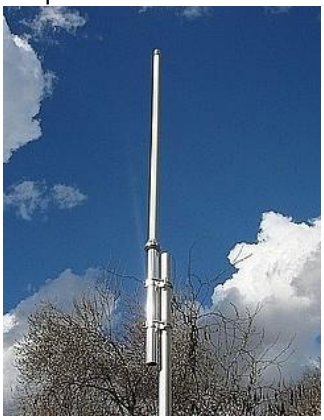


A la fotografia de dalt podem veure una antena tipus Graella WiFi 8/5 GHz, direccional en els 5.8GHz i que treballa amb els protocols: IEEE 802.11b /g WiFi, ISM, bandes NII i WIMAX. Aquest tipus d’antena es pot utilitzar per a sistemes punt a punt, punt a multipunt, Sistemes de vídeo sense fil, 802.11a Wi-Fi xarxes, 802.16 WiMax Xarxes, Hotspots públics sense fil, estacions base.

Antenes Omnidireccionals

Aquestes orienten el senyal en totes direccions amb un feix ampli però de curt abast. Si una antena direccional seria com un focus, una antena omnidireccional seria com una bombeta emetent llum en totes direccions amb menor abast.

Les antenes Omnidireccionals "envien" la informació teòricament als 360 graus pel que és possible establir comunicació independentment del punt en què s'estigui. En contrapartida l'abast d'aquestes antenes és menor que el de les antenes direccionals.



A la fotografia de dalt podem veure una antena tipus Omnidireccional per a enllaços Wi-Fi que que treballa a 2.4 GHz.
Aquest tipus d'antena es pot utilitzar per a sistemes per a cobertura general en pobles i Petites Ciutats. Te un alt Guany Omnidireccional que el fa òptim per a estacions base Wi-Fi amb una recepció de 360 º Viable per Hotspot Públic Wireless, protocols IEEE 802.11b, 802.11gi 802.11n wireless LAN, Bluetooth.

Antenes Sectorials

Aquestes son la barreja de les antenes direccionals i les omnidireccionals. Les antenes sectorials emeten un feix més ampli que una direccional però no tan ampli com una omnidireccional. Per tenir una cobertura de 360 º (com una antena omnidireccional) i un llarg abast (com una antena direccional) haurem instal·lar o tres antenes sectorials de 120 º o 4 antenes sectorials de 80 º. Les antenes sectorials solen ser més costoses que les antenes direccionals o omnidireccionals.

A la fotografia de dalt podem veure una antena tipus Sectorial WiFi de 2.4 GHz d'alt rendiment.
Aquest tipus d'antena es pot utilitzar per a sistemes IEEE 802.11b, 802.11g i 802.11n i les podem veure molts cops penjades a façanes d'edificis, hotels, col·legis, hotspot públic, degut a la seva versatilitat.

Topologies de xarxa

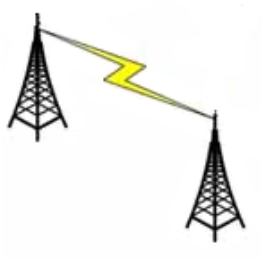
Abordem ara algunes de les topologies bàsiques que trobem als sistemes de comunicacions. Es tracta d'abstraccions que ens permeten observar el flux de la informació sense necessitat d'estar considerant constantment les característiques del medi i tota la resta d'elements involucrats.

Quan ens referim a una determinada topologia, podem utilitzar-la per a representar la forma de connexió i el flux físic de les dades, com per exemple: punt a punt, punt a multipunt o malla.

Punt a punt

Quan parlem d'un enllaç punt a punt, ens referim a un en el qual tota la comunicació es produeix entre dos punts, i nomes estre aquests. El cas mes simple i potser el mes comú es el de la unió de dos equips mitjançant un cable.

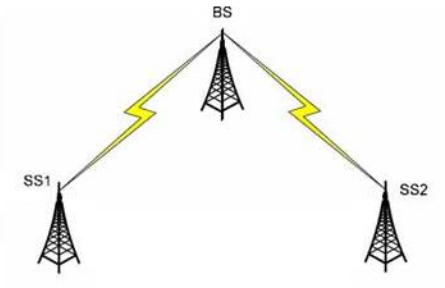
Una comunicació punt a punt half-duplex requereix d'un cable que uneixi tots dos nodes; una comunicació punt a punt full-duplex requerirà de dos cables que uneixin ambdós nodes, o alguna forma en que dos senyals puguin viatjar al mateix temps en sentits diferents pel mateix medi de comunicació, com per exemple modular cada una d'elles amb diferents freqüències de portadores.



Punt a multipunt

En un enllaç punt a multipunt, existeix un punt central que es comunica amb altres punts remots. Generalment això implica que la comunicació es nomes entre el punt central i els remots i des de aquests fins a la central; no existeix comunicació entre els remots.

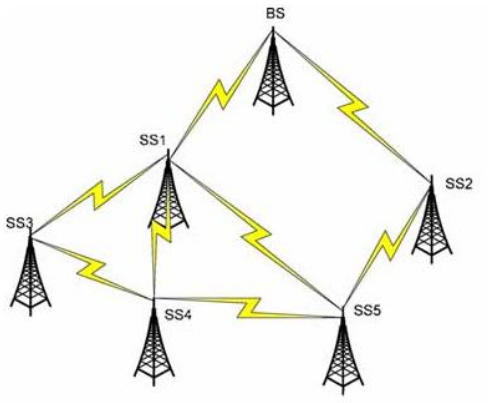
Aquesta topologia generalment implica una comunicació half-duplex, encara que existeixen casos en que s'utilitza una connexió del punt central a tots els remots i una altre compartida pels remots, pel que es possible que el central i un remot parlin a la vegada.



Malla (Mesh)

Un enllaç mallat es una xarxa múltiplement connexa, a la qual els nodes tenen mes d'una connexió amb mes d'un node diferent. No necessàriament han de connectar-se tots contra tots, aquest es un cas especial que es denomina full-mesh, mentre que el cas genèric sol denominar-se partial-mesh, per oposició. En una xarxa full-mesh de n nodes, cada node te una connexió amb els n-1 nodes restants, en un total de n(n-1) connexions. Si be la topologia en sí no implica res, l'ús comú del seu nom fa suposar la existència de Routing de mode que els missatges tinguin possibilitat d'arribar per diferents camins al mateix destí.
Pel tipus de xarxa que volem implantar, dintre de les topologies explicades anteriorment

descartarem la xarxa del tipus malla, degut a que encariria el cost de la xarxa i degut al servei pel qual esta destinada la xarxa no es la millor opció, de la mateixa manera que una xarxa punt a punt també quedaria descartada degut a que no tindrem una connexió única entre dos punts. Per tant utilitzarem la xarxa punt a multipunt ja que pel nostre projecte serà mes eficient i utilitzarem menys accés points, reduint d'aquesta manera sensiblement el cost.



Propagació de Radio Freqüències

Les ones electromagnètiques posseeixen dos components: una elèctrica i una magnètica. Existeixen diferents freqüències d'oscil·lació, mentre la freqüència augmenta, la longitud d'ona disminueix, com ho explica la següent equació:

$$\lambda = \frac{velocitat}{freq\text{üència}}$$

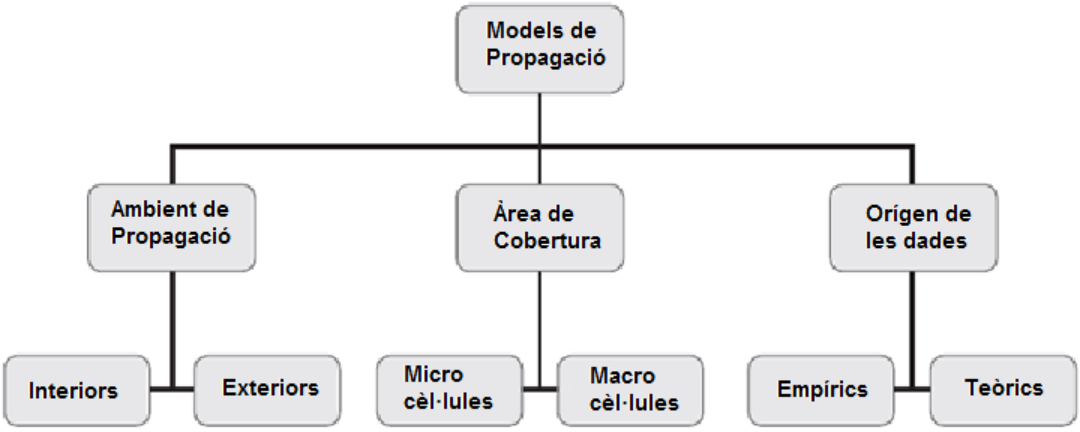
L'espectre de radio freqüències que s'utilitza actualment per a les comunicacions, tant amb fils com a sense, inclouen les freqüències que s'estenen des dels 30Khz fins als 300Ghz, però degut a que a molt altes freqüències les ones son afectades de manera considerable, no s'utilitza el rang de les ones EHF.

Models de propagació

Existeixen diversos models de propagació de Radio Freqüència que ens permeten predir el comportament de les ones, generalment els models de predicció es poden classificar en empírics, teòrics o una combinació d'aquests dos, semi-empírics.

Els models empírics es basen en medicions, i els models teòrics es fonamenten en els principis fonamentals dels fenòmens de propagació d'ones de radio. Els models de propagació prediuen la pèrdua per trajectòria que un senyal de Radio freqüència pugui tenir entre una estació base i un receptor mòbil o fixe. La avantatge de modelar radio canals tenint en compte les característiques de la trajectòria entre Transmissor (Tx) i Receptor (Rx), es conèixer la viabilitat dels projectes que es desitgen planificar en determinats sectors, d'aquesta manera es podrà fer una estimació sobre la necessitat, costos i capacitats dels equips requerits.

Taula de models de propagació

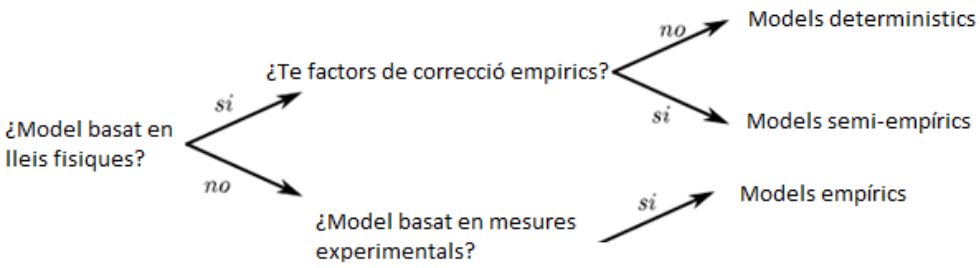


En un principi quan aparegueren les xarxes sense fils s'utilitzaven poques antenes i ubicades a una gran alçada. Aquesta implementació era valida degut a que la demanda pel servei era mínima. Amb l'augment del numero d'usuaris va ser necessari disposar de mes antenes i canals, pel que va se necessari reutilitzar les freqüències, el que va permetre tornar a utilitzar el mateix canal en un altre lloc. Per a disminuir al màxim la interferència en els límits de les cèl·lules es devia obtenir millors prediccions de cobertura. Actualment podem trobar quatre tamanys: Macro, Mini, Micro i pic Cèl·lules.

Tipus de cel·lula	Radio de Cel·lula	Posició de la antena TX
Macro Cel·lula	1 a 30 km	Outdoor, montada sobre el nivell dels sostres, les alçades que l'envolten son menors que aquesta
Micro Cel·lula	0.5 a 5 km	Outdoor, montada a una alçada menor que la majoria de les edificacions, i les que la envolten son mes altes.

Els models que es presenten a continuació estan classificats en teòrics i empírics, en els primers s'ha de tenir major informació sobre la ciutat en particular i la estructura de les edificacions.

Els models empírics es van desenvolupar utilitzant una sèrie de medicions, de les quals es van obtenir les fórmules de propagació.



Models empírics	Models semi-empírics	Models deterministics
Mod. Hata	Mod. Egli	Mod. Friis
Mod. Okumura	Mod. Walfisch	Difracció per objectes prims
Mod. en lleis de potencia	Mod. Ikegami	Mod. dos ratjos
	Mod. Longley Rice	

Aquests models son basics per a entendre els resultats que s'obtindran, en el cas de Wimax els mes utilitzats son:

- Model de Friis (per a espai lliure)
- Model de Okumura
- Model de Hata
- Model Walfisch-Ikegami
- Model Longley-Rice o Irregular Terrain Model (ITM)

Model de Friis (per a espai lliure)

El model de propagació en espai lliure, s'utilitza per a predir el nivell de potencia rebut en una certa ubicació, quan no existeix cap objecte al voltant de l'enllaç que pugui afectar la propagació electromagnètica. Això es una condició molt mes exigent que la coneguda com a "línia de vista" (line of sight, LOS) entre el transmissor (Tx) i receptor (Rx) que nomes considera obstacles en la línia que uneix ambdós element de l'enllaç. Un enllaç pot ser LOS, però això no impedeix que objectes propers produeixin reflexions que puguin afectar la senyal que es propaga en el trajecte directe. El model de propagació d'espai lliure es per una altre banda una bona referencia de comparació per a enllaços mes complexes i es bastant exacte quan l'efecte de elements propers no es significatiu, com passa per exemple en enllaços satel·litals.

El model prediu que la potencia disminueix en funció de la separació "d" entre el Tx i Rx, d'acord a la equació de Friis.

$$P_r(d) = \frac{P_t G_t G_r}{L}\left(\frac{\lambda}{4\pi d}\right)^2$$

On P_t és la potència transmesa, $P_r(d)$ és la potencia rebuda, que és una funció de la separació entre transmissor i receptor, G_t és el guany de l'antena de transmissió, G_r és el guany de l'antena de recepció, d és la separació Tx-Rx en metres, L són les pèrdues del sistema no relacionades a la propagació $L \geq 1$ i λ és la longitud d'ona de la senyal electromagnètica en metres.

Les pèrdues de trajecte (path loss) representen la atenuació de la senyal com a una magnitud positiva, expressada en dB, i estan definides com la diferencia entre la potencia transmesa i rebuda d'acord a la equació:

$$PL(dB) = -20\log(\frac{\lambda}{4\pi d})$$

Val la pena destacar el fet que les equacions anteriors nomes tenen validesa a la regió de camp llunyà o regió de Fraunhofer, es a dir, per a aquelles distancies que superen 2 2 $fd = D\,\lambda$, $f\,d > \lambda$ a on *D* es la major dimensió lineal de la antena de transmissió.

Model de Okumura

És un dels models més utilitzats per a la predicció de la pèrdua de propagació en àrees urbanes. El principal resultat del treball de Okumura va ser un conjunt de corbes que proporcionen el nivell d'atenuació mitja relativa a l'espai lliure, en funció de la freqüència, la distància entre transmissor i receptor, l'alçada de les antenes de la estació base i la estació mòbil, a més a més de varis factors de correcció específics per a diferents tipus de trajecte. Aquest model està considerat entre els més simples i millors en termes de la seva precisió en el càlcul de les pèrdues en el trajecte.

Segons aquest model, la distància màxima de separació que pot existir entre el transmissor i el receptor és de fins a 100 km. Pot ser utilitzat per a altures de la antena de la estació base en el rang de 30m a 1000m. Les pèrdues existents a l'enllaç pot ser obtinguda mitjançant la equació:

$$L_{50}(dB) = L_F + A_{MU}(f,d) - G(h_{te}) - G(h_{re}) - G_{AREA}$$

- L_{50} son les pèrdues de propagació al 50 % de recepció de la senyal.
- L_F pèrdues en espai lliure.
- $A_{MU}(f,d)$ atenuació mitja
- $G(h_{te})$ guany de la antena transmissora (dB)
- $G(h_{re})$ guany de la antena receptora.
- G_{AREA} guany de l'entorn.

Okumura va desenvolupar un set de corbes que entreguen la atenuació relativa a l'espai lliure mig, que és utilitzat com a nivell de referencia, per a zones urbanes sobre terreny quasi pla, en base a extenses medicions, a més a més de basar-se en paràmetres predefinits.

És un dels models mes simples i adequats per a les prediccions d'atenuació per a sistemes cel·lulars i sistemes de ràdio terrestre en ambients poblats, ja que no és tan bo en zones rurals.

Model de Hata

En aquest model s'obté una formula empírica per a les pèrdues per propagació a partir de les medicions fetes per Okumura. El model tracta de representar les medicions fetes per Okumura a través de la forma:

$$A + B\ log10\ R$$

A i B: funcions de la freqüència i l' alçada de la antena
R: distancia entre l'antena i l'usuari.

Amb l'objectiu de fer que aquest model fos mes fàcil d'aplicar, Hata va establir una sèrie de relacions numèriques que descriuen el mètode gràfic proposat per Okumura. Aquestes expressions de caràcter empíric, son conegudes sota el nom de model Okumura-Hata.

El principal resultat que proporciona el model es el valor mitja de la pèrdua bàsica de propagació, en funció de la freqüència, la distancia i les alçades de les antenes de la estació base i el mòbil encara que aquest no inclou cap dels factors de correcció per tipus de trajecte, els quals si estan en el model de Okumura, les equacions proposades per Hata tenen un important valor pràctic.

Les aproximacions fetes per Hata involucren dividir les àrees de predicció categoritzades pel tipus de terreny, anomenades àrea oberta, urbana i suburbana.

Àrea urbana: Correspon a les grans ciutats amb altes edificacions i cases amb 2 o mes pisos, a on existeixen una gran concentració de cases.
Àrea suburbana: Ciutats o carreteres a on hi ha arbres i cases en forma dispersa, existeixen obstacles a prop de l'usuari però no provoca congestió.
Àrea oberta: Son els espais oberts sense grans arbres o edificacions en el camí de la senyal.
Les aproximacions fetes per Hata tenen validesa dintre dels límits dels paràmetres de la taula.

Paràmetres	**Rang de Validesa**
Freqüència (f) en [Mhz]	100-1500
Alçada efectiva de la estació base (h_b)en [m]	30-200
Alçada de la antena del mobil (h_m)en [m]	1-10
Distancia (R) en [Km]	1-20

Model Walfisch-Ikegami

Aquest model es basa en els models de Walfisch i Ikegami per a predir les pèrdues.

Es tradueix en la suma de les pèrdues per espai lliure Lb amb les pèrdues dels models de Ikegami, i un model estes de Walfisch-Bertoni. Tenim per al LOS:

$$L_b = 42.6 + 26 \log d + 20 log f$$

Les pèrdues totals es computen per al cas NLOS:

$$L_{COST} = L_{FREE} + \begin{Bmatrix} L_{rts} + L_{msd} & si\ L_{rts} + L_{msd} > 0 \\ 0 & si\ L_{rts} + L_{msd} < 0 \end{Bmatrix}$$

$A\ on\ L_{rts}$ són les pèrdues del model de Ikegami (Roof to Street) i a l'altre cas les pèrdues del model de Walfisch (multiple screen diffraction).

Model Longley-Rice o Model Irregular Terrain Model (ITM)

El model Longley-Rice prediu la possible propagació a llarga-mitja distància sobre el terreny irregular. Va ser dissenyat per a freqüències entre els 20MHz y 20GHz, per a longituds de trajecte d'entre 1 i 2000 Km.

També és un model estadístic però te en compte molts mes paràmetres per al càlcul de les pèrdues:

- Alçada mitja del terreny (ondulació)
- Refracció de la troposfera
- Perfils del terreny
- Conductivitat i permissivitat del sòl
- Clima

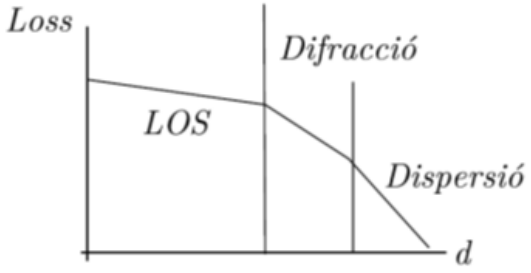
Per al càlcul de la propagació, el model Longley-Rice te els següents paràmetres comuns al de altres models de propagació:

- Freqüència: el rang de freqüències nominals pel model varia entre 20MHz i 20GHz.
- ERP (Effective Radiated Power): potència efectiva de radiació, s'introdueix en les unitats que fixa l'usuari en la opció de configuració del sistema (mW, W, kW, dBm, dBW, dBk).
- Polarització: ha de especificar-se si es treballa amb polarització horitzontal o vertical. El model de Longley-Rice assumeix que totes les antenes tenen la mateixa polarització.
- Refractivitat: la refractivitat de l'atmosfera determina la quantitat de "bending" o curvatura que sofriran les ones radio. El paràmetre de refractivitat típic de la Terra és 4/3 (1.333) que correspon a una refractivitat de superfície de valor aproximadament a $N_s = 301$ Unitats de n. En general, el promig de refractivitat decreix amb l'altitud, començant amb el seu valor màxim al nivell del mar.

De manera que el factor k multiplicat pel radi terrestre de la Terra. La relació entre els paràmetres K i N , ve donada per la següent expressió:

$$N_S = 179.3 * Ln\left[\frac{1}{0.046665}\left(1 - \frac{1}{K}\right)\right]$$

Pel càlcul de les pèrdues el model utilitza la teoria de la difracció, la refracció troposférica i el escatering del terreny. Les pèrdues addicionals estan basades en mesures agafades en vàries situacions.



El Model Irregular Terrain Model (ITM), s'utilitza en els programes Radio Mobile i OPNET, i encara que és més comú per a calcular enllaços punt a punt, també es pot utilitzar per a modelar WIMAX i propagació de ràdio freqüències.
Radio Mobile permet fer un anàlisi de cobertura, o de predicció d'àrea, aquest tipus d'anàlisi no treballa sobre una trajectòria determinista, sino que genera una projecció del àrea a cobrir a partir de la terminal donant les característiques de cada ràdio-base o antena i les irregularitat del terreny.

Relació d'Ones Estacionaries

Quan una línia de transmissió porta potència a una càrrega (antena) que no la dissipa completament diem que la línia té una component reactiva , que té entre les seves característiques tornar potència a la font emissora (equip de ràdio). Aquesta potència retornada s'anomena component reflexada (reflected power en anglès) que flueix en sentit contrari a la component directa (forward power en anglès , la que va del transmissor de ràdio a l'antena) i com hi ha dues ones que flueixen en sentit contrari , aquestes produeixen ones estacionàries en la línia de transmissió.

La relació entre els valors màxims i mínims de tensió (voltatge) de RF en la línia s'anomena ROE (relació ones estacionàries o standing wave ràtio SWR en anglès) i pot indicar , entre altres coses , una desigualtat d'impedància entre la línia de transmissió i la càrrega (antena) .

La línia de transmissió té una impedància característica que ha de ser adaptada a la impedància de l'antena per evitar les ones estacionàries . També la impedància de la línia de transmissió ha d'estar adaptada a la impedància del transmissor. Es pot usar un acoplador d'antena (antenna tuner en anglès) per acoplar la impedància del sistema d'antena (línia de transmissió i antena) a la impedància de sortida transmissor (output impedance en anglès) perquè el transmissor *vegi* la càrrega en el sistema d'antena i hagi transferència total de potència del transmissor al sistema d'antena .

És important, comentar que els equips transmissors escollits per al projecte, redueixen automàticament la seva potència en augmentar el valor de la relació ones estacionàries . Perquè tot el sistema funcioni perfectament, el transmissor, la línia de transmissió i l'antena han de tenir la mateixa impedància o estar acoplats .

També és molt important que l'antena tingui les dimensions necessàries per a la banda en la qual s'usa i que la impedància de l'antena sigui igual a la impedància de la línia de transmissió .

Per exemple , si alimentem una antena de 50 ohms d'impedància (dipol de mitja ona) amb una línia de transmissió de la mateixa impedància (coaxial) i ambdues impedàncies estan acoplades, tindrem una SWR (relació d'ones estacionàries) de 50/ 50 o sigui 1:1 . Però si alimentem una antena de 200 Omhs amb una línia de transmissió de 50 ohms , la relació ones estacionàries o SWR serà 200/50 o sigui 4:1, aquí no hi ha acoplament d'impedàncies . En aquest últim exemple hi ha pèrdues en la línia de transmissió per reflexions múltiples del senyal entre l'antena i el transmissor ja que cada vegada que la potència transmesa ha de viatjar per la línia de transmissió, part de l'energia es dissipa com a calor.

A la taula es mostra la variació d'energia efectiva radiada des de la antena quan canvia el ROE.

* PER = Percentatge de la potencia efectiva radiada

ROE MESURADA	% DE PÉRDUDA	PER*	POTENCIA (WATTS)
1.0:1	0.0%	100.0%	4.00
1.1:1	0.3%	99.7%	3.99
1.2:1	0.8%	99.2%	3.97
1.3:1	1.7%	98.3%	3.93
1.4:1	2.7%	97.3%	3.89
1.5:1	3.0%	97.0%	3.88
1.6:1	5.0%	95.0%	3.80
1.7:1	6.0%	94.0%	3.76
1.8:1	8.0%	92.0%	3.68
2.0:1	11.0%	89.0%	3.56
2.2:1	14.0%	86.0%	3.44
2.4:1	17.0%	83.0%	3.32
2.6:1	20.0%	80.0%	3.20
3.0:1	25.0%	75.0%	3.00
4.0:1	38.0%	62.0%	2.48

Equips escollits

Finalment i després de comparar entre varies marques pioneres i reconegudes en el mercat de les telecomunicacions com son Cisco, Alvarion, Selesta Networks, Unidata, Tranzeo, Telsa.

Ens hem decantat per Albentia Systems ja que es la primera empresa a nivell mundial en fabricar una BS completament Inter operable i compatible al 100% amb l'estàndard IEEE 802.16. Això vol dir que pot funcionar amb un gran rang de CPEs d'altres marques.

Per tant, la interoperabilitat amb altres CPEs d'altres fabricants es un valor afegit importantíssim, ja que determinades marques de CPE només poden "parlar" amb les BS del mateix fabricant. La interoperabilitat garantitza una major possibilitat de decisió i permet utilitzar el CPE que mes s'adapti a les nostres aplicacions, on prima el baix cost i les prestacions professionals entre d'altres.

Ens hem decantant per comprar el servidor de la marca Dell, degut a que la seva gama de servidors PowerEdge esta dissenyada per a proporcionar la flexibilitat, escalabilitat i formats necessaris per a un petit municipi.

En quant al tallafocs, la opció escollida ha esta el fabricant , palo alto networks degut a la capacitat d'identificar aplicacions, usuaris, protegir contra virus, spyware i atacs, entre altres.

Radioenllaç ARBA Link-350

El radioenllaç escollit ha estat el model ARBA Link-350 de la nova família de radioenllaços punt a punt IP 802-16 de Albentia Systems. Ofereix extraordinària capacitat de fins a 300 Mbps en bandes no llicenciades de 5 GHz. Les solucions punt a punt ARBA Link cobreixen tot tipus de necessitats, es poden emprar com a simples bridges sense fils o com a un sistema de backhaul d'accés WiMAX.

Imatge del model ARBA Link – 350 (radioenllaç punt a punt)

Foto real de l'antena de Camprodon on instal·larem l'equip.

Estacions Base ARBA PRO-BS-1400

ARBA PRO-BS-1400 es l'equipament sense fils punt a multipunt desenvolupat per Albentia Systems per a aplicacions professionals i mercats verticals.

Pot arribar a suportar fins a 140 Mbps reals per sector, ofereix una extraordinària eficiència espectral i potents mecanismes de seguretat.

Característiques principals:

- Fins a 140 Mbps per sector
- Full-outdoor IP67
- Capacitat garantitzada per subscriptor i servei diferenciat
- OFMD MIMO 2x2 amb diversitat espacial i freqüencial
- Xifrat AES128 i certificats X.509 per a màxima seguretat
- Banda de 4.9-5.875 GHz
- Llarg abast: > 50 km
- Baixa latència < 5ms

Les especificacions tècniques de l'equip es poden observar en l'annex d'aquest document, nomes destacaré algunes característiques.

Bandes de freqüència:	4.9 GHz, 5.9 GHz
Ample de banda de canals:	20MHz
Potencia de Transmissió:	29 dBm
Ganancia de antena integrada:	Connector N, 20/23dBi
Capacitat real màxima	140 Mbps
Interfaç de dades:	Ethernet 10/100 Base-T
Consum de Potencia:	<18W

Imatge del model ARBA PRO-BS-1400 (estació base)

Unitats Subscriptores ARBA PRO-SU-1200

Albentia Systems ofereix una gama de CPEs que permet cobrir totes les necessitat de desplegament en xarxes d'accés sense fils. ARBA PRO-SU-1200 està dissenyat per a cobrir els exigents requeriments dels usuaris, en termes d'aspecte mecànics, ambiental i de capacitat. Per a la instal·lació de l'equip únicament es necessària una connexió a una Font de CA o CC.

Bandes de freqüència:	4.9 GHz, 5.9 GHz
Ample de banda de canals:	10MHz
Potencia de Transmissió:	29 dBm
Ganancia de antena integrada:	Connector N, 20/23dBi
Capacitat real màxima	70 Mbps
Interfaç de dades:	Ethernet 10/100 Base-T
Consum de Potencia:	<10W

Imatge del model ARBA PRO-SU-1200 (unitat subscriptora)

AP-24-8: 2.4GHz Outdoor Access Point

AP-24-8 es una solució d'accés sense fils amb capacitat d'actuar com a AP o CPE proporcionant o una connectivitat sense fils fiable per a entorns rurals. El seu injector PoE el dota de major flexibilitat per al desplegament en llocs en els que no hi ha alimentació en DC disponible. El AP-24-8 es totalment compatible amb l'estàndard IEEE 802.11n, pel que ofereix tres vegades mes velocitat de transmissió que els dispositius 802.11g convencionals.

Per a protegir la privacitat dels usuaris i garantitza la seguretat de les dades, el AP-24-8 implementa les últimes tecnologies de xifrat com WPA2/WPA/802.1x dotant a la seva xarxa de potents mesures de seguretat i autenticació.

Les seves principals característiques son:

- Conformitat als estàndards IEEE 802.11b/g/n
- Fins 600mW (26dBm)
- Seguretat Inhalàmbrica WPA / WPA2
- Compleix RoHS
- Potencia de transmissió ajustable
- Chipset: Família Atheros AR9002
- Tecnologia Atheros Align
- Sortida de RF seleccionable per SW: Antena integrada 8dBi o Connector N mascle

Imatge del model AP-24-8: 2.4GHz Outdoor Access Point (punt d'acces WIFI)

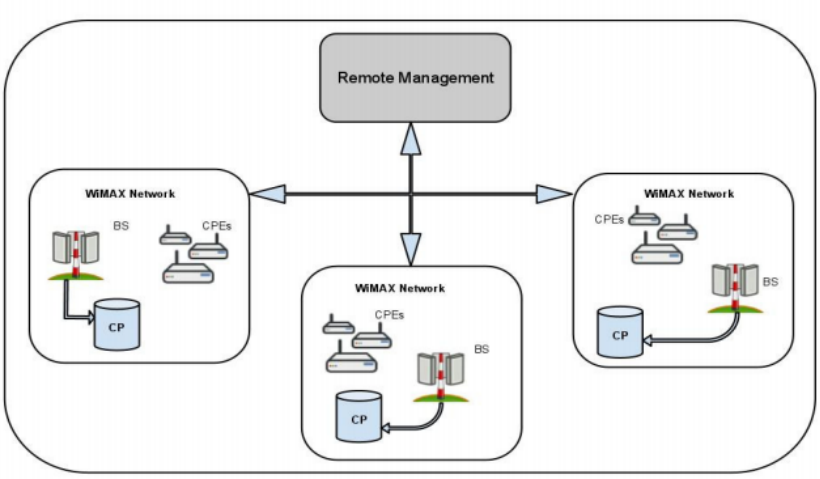
Per tal de proveir de zones Wifi a diferents llocs públics del poble, col·locarem nous CPEs que incloguin un Hot Spot Wifi a la mateixa carcassa i creïn rangs de cobertura Wifi de cents de metres de cobertura.

Imatge del model AP-24-8: 2.4GHz Outdoor Access Point instal·lat a una mastil

Sistema de provisió centralitzada CPS

A la nostra xarxa amb múltiples estacions base les quals donen servei a gran numero d'usuaris podem optimitzar la gestió mitjançant el CPS (*Central Provisioning System*). Aquesta eina proporciona una base de dades centralitzada i replicable, a la qual les estacions base consulten les peticions d'access dels clients així com els serveis que tenen contractats.

Imatge de la Integració del CPS a la xarxa de l'ajuntament



Sistema de gestió de xarxa AMS - AAS (as a Service)

L'eina AMS (Advanced Management System) es un sistema de gestió de xarxa avançat per a solucionar les necessitats d'operació i manteniment de les xarxes d'acces i esta adaptat a les particularitats d'una xarxa d'accés sense fils. Amb funcionalitat Full FCAPS, permet al operador reduir els seus costos de manteniment i operació.

Continuant amb la tendència del mercat d'aplicacions empresarials, contractarem el model gestionat al núvol.

Les principals avantatges d'aquest sistema son:

• No hi ha necessitat d'inversió en equipament, ni en llicencies de software.

• L'operador no ha de dedicar recursos personals ni materials al manteniment i el sistema sempre esta actualitzat a la ultima versió.

Servidor Dell PowerEdge R210 II

Aquest servidor muntarà la base de dades del sistema de provisió centralitzat CPS, Radius i el servei de hotspot, i el servei de DHCP (entregarà automàticament una ip lliure al equip).

Algunes característiques que podem destacar:

- Model: PowerEdge R210 II Chassis, 2x3.5" Cabled HDDs
- Procesador Intel® Xeon® Processor E3-1280v2, 4C/8T, 3.60GHz, 8M Cache, 69W TDP, Turbo Memoria: 8GB Memory (1x8GB) 1600Mhz Dual Ranked Low Volt UDIMM
- Sistema operatiu instal·lat de fàbrica: Windows Server 2008 R2 SP1
- Primera unitat de disc dur: 500GB, SATA, 3.5-in, 7.2K RPM

Servei Radius

L'Autenticació remota telefònica d'usuari Service (RADIUS) és un protocol de xarxa que proporciona autenticació centralitzada , autorització i comptabilitat de gestió (AAA) per als usuaris que es connecten i utilitzen un servei de xarxa .

A causa de l'ampli suport i la naturalesa ubiqua del protocol RADIUS , que s'utilitza sovint pels proveïdors d'Internet i les empreses per gestionar l'accés a Internet o xarxes internes , xarxes sense fils i serveis de correu electrònic integrada. Aquestes xarxes poden incorporar mòdems DSL , punts d'accés , VPN , ports de xarxa , servidors web , etc

RADIUS és un protocol client / servidor que s'executa en la capa d'aplicació , usant UDP com a transport . El servidor d'accés remot , el servidor de xarxa privada virtual , l'interruptor de la xarxa amb l'autenticació basada en el port i el servidor d'accés a xarxa (NAS), són tot utilitzats com a passarel·les que controlen l'accés a la xarxa , i tots tenen un component de client RADIUS que es comunica amb el RADIUS server.

El servidor RADIUS utilitza el concepte AAA per gestionar l'accés de xarxa en el següent procés de dos passos, també coneguda com una "transacció AAA". AAA significa "l'autenticació, autorització i comptabilitat".

El servidor RADIUS és usualment un procés de fons que s'executa en un servidor Microsoft Windows 2008 en el nostre cas, ubicat al Servidor Dell PowerEdge R210 II que tenim a l'ajuntament.

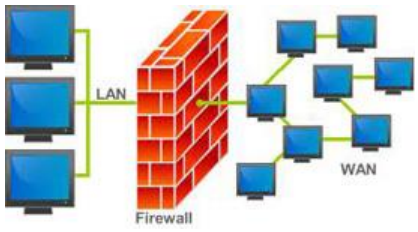
Firewall Palo Alto PA-2050

Un dels temes de mes interès es el de la seguretat dels equips i les dades, essent de vital importància mantenir-nos actualitzat en les noves tecnologies i els nous sistemes per a protegir els nostres equips de qualsevol tipus d'atac electrònic.

Entre els sistemes mes coneguts i de major popularitat en el mon, es troba el Firewall.

És de gran utilitat per a monitoritzar l'accés als nostres equips, així com per a seleccionar que connexions son permeses cap alls nostres equips des de internet.

Imatge representativa de la funció del firewall



El Firewall funciona com a una espècie de barrera entre el nostre equip i Internet i altres xarxes publiques, tancant els ports necessaris segons els nostres requeriments de seguretat.

Per suposat, que l'usuari del Firewall ha de donar una ordre o crear una llista de programes permesos per a realitzar connexions remotes (com l'antivirus). Ja que si el programa no es troba en un llistat d'aplicacions el Firewall no permetrà el seu accés al nostre equip. Serveix de gran utilitat davant dels atacs informàtics, minimitza el risc, ja que impedeix el tràfic d'alguns protocols utilitzats per ciberdelinqüents per a obtenir el control dels equips o infectant els mateixos.

Una de les seves funcions també es evitar que aplicacions externes o estranyes puguin connectar-se als nostres equips i si la seva configuració es correcta, pugui inclús evitar que algun malware realitzi connexions cap als nostres equips.

La configuració del Firewall es de vital importància per a estar protegits davant d'amenaces, però també ho es el sentit comú. Es recomanable evitar donar accés a programes desconeguts i obrir arxius adjunts complementant el Firewall amb un bon antivirus.

El firewall s'encarregarà de controlar tot el tràfic sortint i entrant de la xarxa. Dintre de diversos fabricants s'ha escollit el model Palo Alto PA-2050, que es referent mundial de seguretat en Internet. Ofereix solucions de seguretat total caracteritzades per un Gateway unificat, agent únic endpoint i una única plataforma de seguretat unificada i adaptables per a complir les nostres necessitat. Aquesta combinació es única i es el resultat del seu consolidat lideratge i innovació en els mercats de firewall corporatiu, firewall personal, seguretat de les dades i VPN.

Imatge del model Firewall Palo Alto PA-2050 (tallafocs)

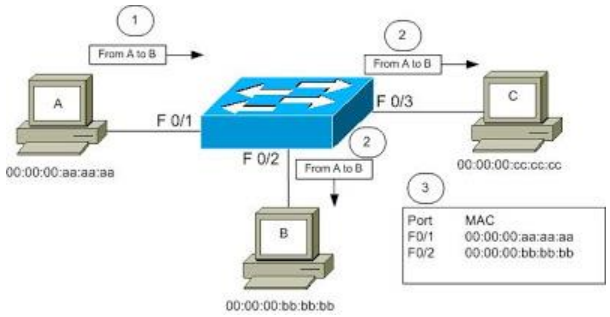
Les seves principals característiques son:
1 Gbps firewall throughput (App-ID enabled[1])
500 Mbps threat prevention throughput
300 Mbps IPSec VPN throughput
250,000 max sessions
15,000 new sessions per second
2,000 IPSec VPN tunnels/tunnel interfaces
1,000 SSL VPN Users
10 virtual routers
1/6* virtual systems (base/max[2])
40 security zones
5,000 max number of policies

Cisco Switch Catalyst 2960-48PST-L

Un Switch es un dispositiu de xarxa que funciona a la capa dos del model OSI, es important saber que la capa 2 te ha veure amb la adreça física de la tarja de xarxa, això es la adreça MAC, que es un numero únic assignat pel fabricant a la tarja de xarxa, cada fabricant te el seu propi rang d'adreces MAC, el que assegura que no es repeteixin.
També hi ha switches de capa 3 i inclús de capa 4, encara que aquests switches mes avançats, han de complir amb les funciones de switch de capa 2.
Un switch ha de realitzar tres tasques bàsiques, les quals es descriuen a continuació:

1. Aprendre adreces (address learning)

El switch té una taula d'adreces MAC amb el port associat, quan el switch s'encén per primera vegada , aquesta taula és buida, suposem que A, desitja comunicar-se amb B, per això, A té preparat un frame, en el qual entre altres coses, te expressades les adreces d'origen i destí. El switch rep aquest paquet i pren nota de l'adreça d'origen i la anota a la taula d'adreces MAC, això és la línia 1 de la taula MAC. Inicialment el switch no coneix on està ubicat B, de manera que reenvia el frame a través de tots els ports excepte en el port on el va rebre, d'aquesta manera B rep el frame i el respon novament amb un paquet que té com a origen la adreça MAC de B, de manera que, el switch ara pot determinar on està ubicat B i afegeix la segona línia de la petita taula MAC. Per a la següent comunicació entre A i B , el switch coneix la ubicació exacta de tots dos i reenvia els frames directament entre A i B.



2. Reenviar i Filtrar

El switch rebrà un frame, examinarà la destinació i buscarà a la taula el port de sortida i l'enviarà únicament a través d'aquest port. Aquesta és la funció del filtre, limita l'enviament del frame al port específic en què es troba el destí. D'altra banda, si la taula MAC encara no té la informació el paquet és reenviat a tots els ports excepte al port en què es va rebre el paquet originalment, el mateix passa quan hi ha un broadcast, és a dir, quan un PC envia un frame de broadcast, aquest és rebut per tots els PCs en el mateix segment de xarxa, en el cas dels broadcast, el switch els reenvia per tots els ports, excepte en el port que el va rebre originalment.

3. evitar Loops

Una tercera funció bàsica i important d'un switch és evitar loops (bucle en anglès, perquè em sembla més apropiat que bucle, o llaç). Per entendre que és un loop, i el perjudicial que és per a qualsevol xarxa. Suposem que per conveniència algú decideix que vol tenir dos enllaços a un mateix switch, de manera que si un falla l'altre funcioni, o suposem que algú inadvertidament veu un cable penjant i amb la millor de les intencions decideix connectar al switch sense adonar-se que aquest mateix cable ja estava connectat en un altre port del mateix switch, el que passa a continuació és desastrós.

El switch l'utilitzarem com a equip d'interconnexió entre els diferents equips emissors de la BS i el Firewall. Al switch es a on crearem les xarxes virtuals, per tal de tenir totalment aïllades les xarxes dels veïnats.

El switch utilitzat serà del fabricant Cisco i aquestes son algunes de las característiques principals:

- Pots: 48x 10/100Base-TX
- altres ports: 2 ranures SFP
- Apilable: no
- Gestionable: sí
- Disseny: rack
- Font d'alimentació: interna
- PoE:sí

Imatge del model Switch Catalyst 2960-48PST-L (concentrador)

Com que a la nostra xarxa tindrem nou AP's crearem diferents Vlans per tal de disminuir els paquets de col·lisió que ens trobaríem en el cas de no comptar amb cap subxarxa. Per aquesta raó, hem optat per la utilització d'un switch de capa 3, la qual cosa ens permetrà avantatges com són el poder enrutar tràfic entre les diferents VLANs que tindrem, filtratge de tràfic no desitjat així com el bloqueig de equips connectats.

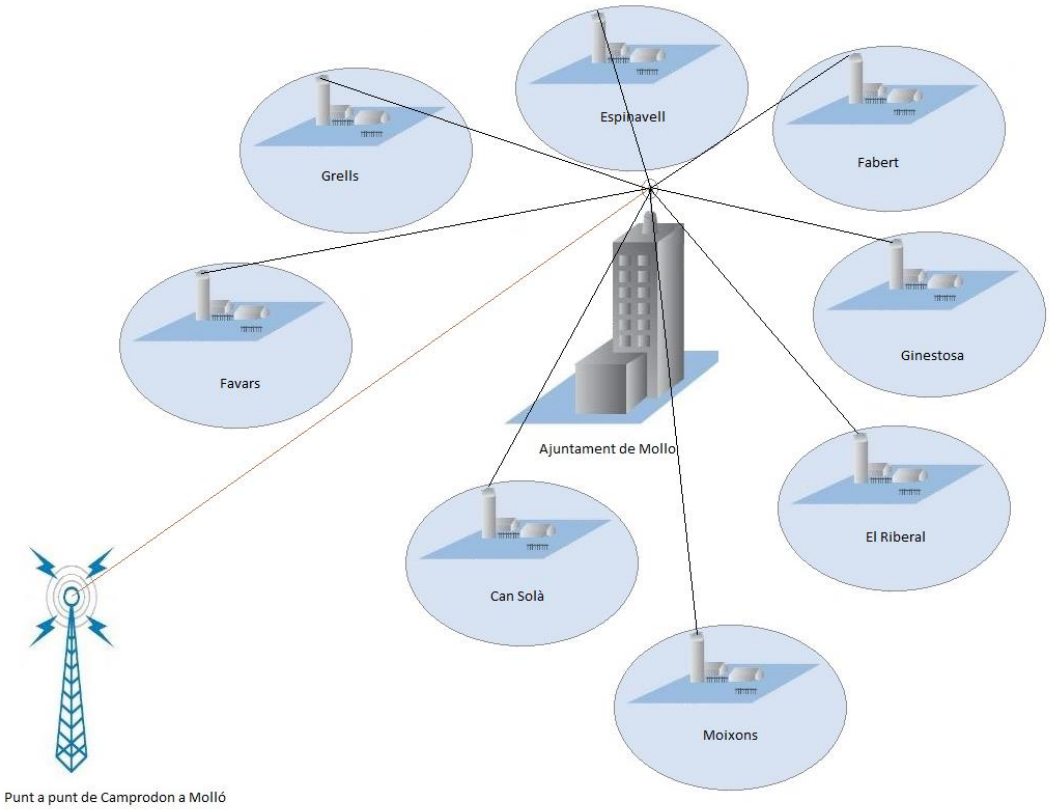
Hotspot (Generador de punts d'accés)

Els Hotspots són els llocs que ofereixen accés Wifi, que poden ser aprofitats especialment per dispositius mòbils com notebooks, PDA, consoles, per accedir a internet. Generalment són un servei que ofereixen els restaurants, hotels, aeroports, shoppings, supermercats, universitats i altres llocs públics . Els hotspot Wifi va ser proposat per Brett Stewart en la conferència Networld / INTEROP a San Francisco a l'agost de 1993 . Si bé Stewart no va emprar el terme *Hotspot,* sí que es va referir a l'accés públic a xarxes LAN sense fils. El terme *HotSpot es* probable que hagués estat proposat per Nokia uns 5 anys després que Stewart el proposes.

Alguns models de WPA es poden utilitzar per a *Hotspot* i suporten un nivell d'autenticació mitjançant RADIUS i altres servidors d'autenticació. Els últims models utilitzen nivells de xifrat de segona i tercera generació, atès que la primera generació de xifrat WEP va resultar bastant fàcil de "crakear".

Aquests nous nivells de xifrat, tant WPA com WPA2, són considerats segurs si la contrasenya és prou forta o bé si s'utilitza "passphrase" (contrasenya formada per frase de pas).

Escenari de xarxa dels diferents veïnats



Simulació i configuració dels equips amb Radio Mobile

Per tal de portar a terme la simulació i configuració dels equips del radio enllaç farem servir l'eina Radio Mobile versió 11.4.2 en anglés. Encara que existeix la traducció a diferents idiomes he preferit no fer servir aquesta capa de traducció ja que hi manquen algunes funcions per traduir o no son traduïdes del tot correcte.

Radio Mobile es un programa de simulació de radiopropagació gratuit desenvolupat per Roger Coudé per a predir el comportament de sistemes de radio, simular radioenllaços i representar l'area de cobertura d'una xarxa de radiocomucinaciones entre d'altres funcions.

Aquesta eina ens permetrà determinar i tenir una representació clara del nivell de propagació que tindrem a Molló un cop distribuïdes les estacions subscriptores, la estació base i els punts d'Access wifi.

El software treballa en el rang de freqüències entre 20 MHz i 20 GHz i esta basat en el model de propagació ITM(Irregular Terrain Model) o model Longley-Rice.

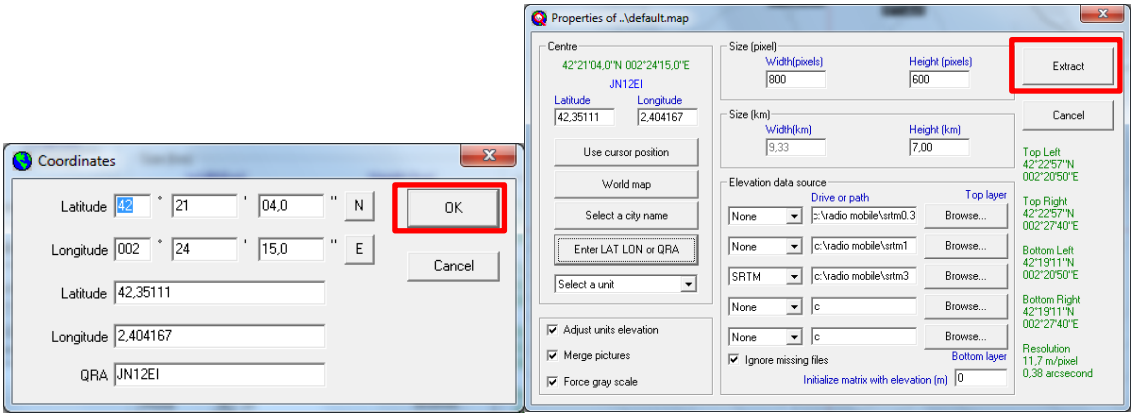
Radio Mobile utilitza dades d'elevació del terreny que es descarregan gratuitament d'Internet per a crear mapes virtuals de l'àrea d'interés, vistes estereoscòpiques i vistes en 3-D.

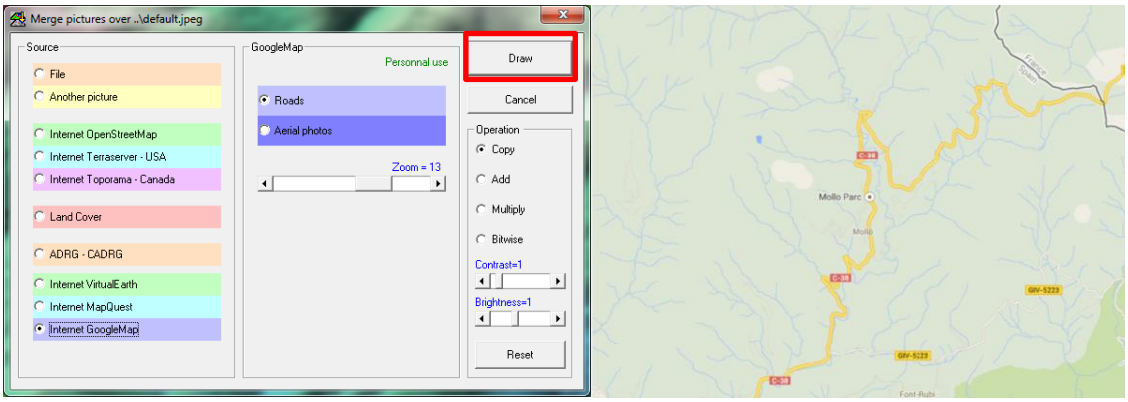
A l'hora d'escollir una eina per fer un estudi de cobertura complert , hem descartat altres productes que hi ha al mercat, com per exemple: Ekahau HeatMapper [3], ja que aquest programari, només es focalitza en mostrar la cobertura Wifi d'un plà, localitzar tots els punts d'accés i detectar les configuracions de seguretat de les xarxes disponibles.

També hem descartat altres eines com Iperf [4], amb la qual es pot analitzar la velocitat de transmissió real en un punt o eines comercials creades per companyies com ara VeriWave amb el seu producte WaveDeploy [5], que permeten una avaluació del rendiment segons l'aplicació, podent realitzar estudis de cobertura no sobre la base de potència rebuda, sinó sobre la qualitat de vídeo o veu que es pot obtenir en un punt

Mapa

Per a la realització d'aquesta simulació he fet servir un mapa d'elevació de terreny de Molló, proporcionat per la mateixa eina, un cop posades les coordenades de latitud i longitud el programa centra un punt i extreu el mapa corresponent a l'àrea indicada, permeten escollir entre diferents repositoris i tipus de mapes.





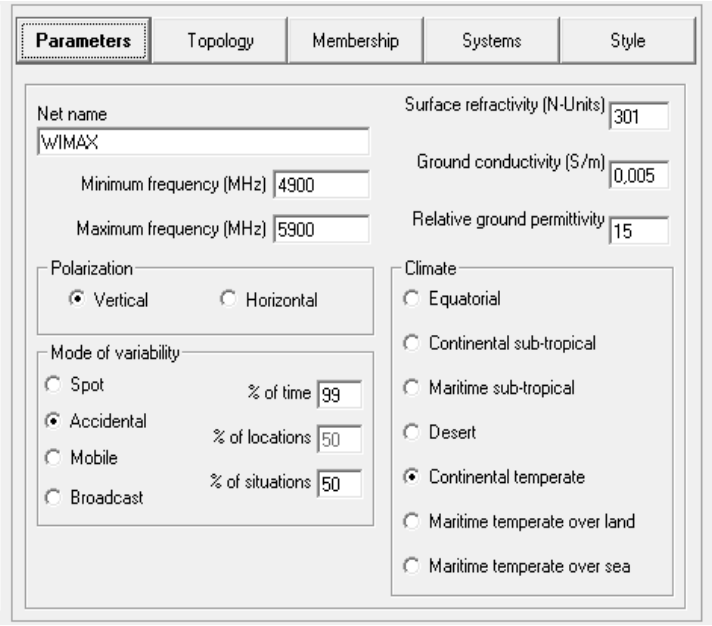
En el nostre cas escollirem el repositori de mapes de google maps i la combinació del mapa de carreteres i el de fotos aeries ja que treballarem posteriorment amb google earth i d'aquesta manera asegurarem que les latituds i longituds estan relacionades de la mateixa manera i conservem la veracitat de les dades un cop exportades.

3 http://www.ekahau.com/wifidesign/ekahau-heatmapper
4 http://iperf.fr/
5 http://www.ixiacom.com/wavedeploy/

Paràmetres globals.

Els paràmetres globals fan referencia a les freqüències de treball, el tipus de terreny, el clima, la polarització de les antenes i el mode de variabilitat. Dintre de *Networks properties – Parameters* apareix la següent finestra:

Paràmetres globals de la xarxa



El primer pas es assignar-li un nom a la xarxa en el camp *Net name.* En el nostre cas es tindrem diferents xarxes: *Wimax, Wifi, i Radioenllaç Camprodon-Molló.*

Canviarem les freqüències mínimes i màximes en funció de la xarxa a l'exemple he treballat amb la freqüència Wimax (4,9-5,9 Ghz), sent la mateixa freqüència per al Radioenllaç, però per a la xarxa Wifi, treballarem a 2,4 Ghz (2,412-2,472 Ghz).

- "Mínimum frequency (MHz)": llindar inferior de la banda de freqüències per a la que es realitzaran els càlculs. En el nostre cas ens centrem a la banda de 4900 Hz
- "Maximum frequency (MHz)": llindar superior de la banda de freqüències per a la que es realitzaran els càlculs. En el nostre cas ens centrem a la banda de 5900 Hz

La resta de camps fan referencia als següents paràmetres i seran els mateixos per a les diferents xarxes que hem creat:

- "Surface refractivity (N-Units)": refractivitat de la superfície terrestre en funció de la refractivitat a nivell del mar i de la altitud mitja del terreny. El valor per defecte (301) es considera adequat en quasi tots els casos.
- "Ground conductivity (S/m)": conductivitat del terreny, expressada en Siemens per metre. Depèn del tipus de terreny i de la freqüència de treball. A la nostra àrea de treball la conductivitat del sòl es de 0,005 S/m.
- "Relative ground permitivity": permitivitat relativa del terreny. Depèn del tipus de terreny i de la freqüència de treball. La permitivitat relativa del terreny es igual a 15.

“Polarization (Vertical)”: Polarització de las antenes empleades a la xarxa. La polarització vertical es la utilitzada normalment en els enllaços de radio de les bandes de VHF i UHF, ja que les ones de radio amb aquesta polarització sofreixen menor atenuació a la superfície terrestre que les que tenen polarització horitzontal.

“Mode of variability”: Longley - Rice defineix quatre modes de variabilitat . La manera seleccionat determina el significat dels valors de fiabilitat i confiança utilitzats en el model. La manera de variabilitat pot ser considerat com el "punt de vista " per considerar el significat de "fiabilitat " i "confiança" en els càlculs.

- El mode *Spot* (manera d'un sol missatge) és un missatge d'un intent.
- El mode *Accidental* (individualment) és per avaluar la interferència.
- El mode *Mobile* és per unitats que es mouen mentre es comuniquen.
- El mode *Broadcast* és per a unitats fixes.

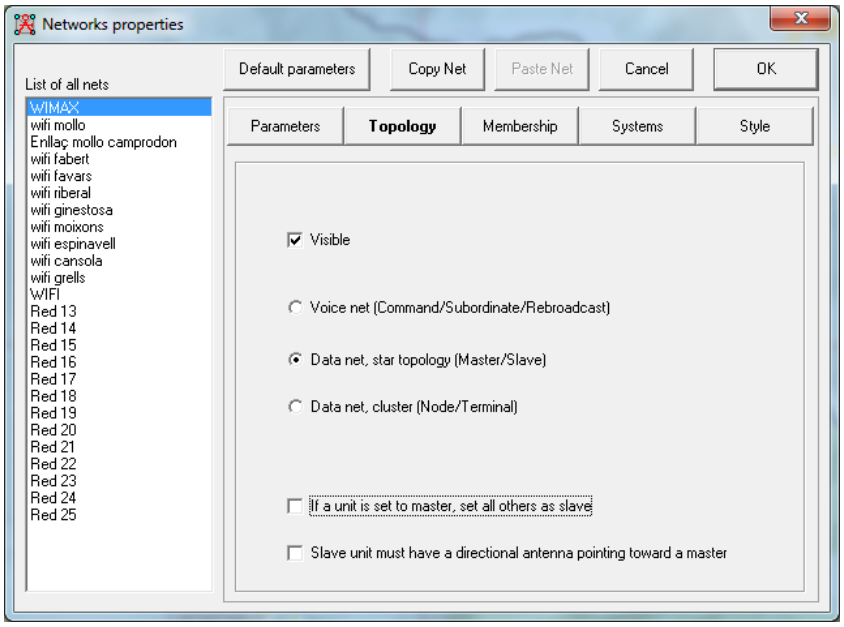
Segons el mode que escollim podrem variar la casella de tant percent de *time, locations i situations* de la part dreta del recuadre.

“Climate”: Les condicions atmosfèriques com el clima i el temps varien en les diferents regions del món , i afecten tant l'índex de refracció de l'aire lliure i jugar un paper important en la determinació de la resistència a la decoloració i les propietats dels senyals de ràdio. Per exemple , el gradient de l'índex de refracció de l'aire prop de la superfície de la terra determina la manera , un raig de ràdio està doblada o refractada quan passa a través de l'atmosfera . En el nostre cas escollirem un tipus de clima Continental Temperat , comú a les grans masses de terra a la zona temperada.

<u>Topologia de la xarxa</u>

En aquest apartat definirem la topologia de la xarxa de radiocomunicacions. Dintre de “Networks properties –Topology**”:**

Topologia de la xarxa



Seleccionem la xarxa de treball a la part Esquerra (Wimax en el nostre cas) i configurem els següents paràmetres:

"Visible": si està marcat, fa que la xarxa sigui visible en el mapa de treball.

- "Voice net (Command / Subordinate / Rebroadcast)": s'utilitza aquesta opció per a xarxes en las que la comunicació es realitza entre una estació de referencia i varies estacions subordinades, sense que hagi radioenllaç addicionals entre estacions subordinades. Es el cas d'una xarxa privada mòbil amb un repetidor que dona servei a varies estacions mòbils, o també d'una xarxa digital amb salt en freqüència en la que la base de temps la proporciona una estació directora.
- "Data net, star topology (Master/Slave)": S'utilitza aquesta opció per a xarxes de dades en las que una estació mestra controla a varies estacions subordinades, sense que existeixin radioenllaç directe entre aquestes ultimes.
- "Data net, cluster (Node/Terminal)": s'utilitza aquesta opció per a xarxes de dades que puguin retransmetre datagrames (*digipeaters*).

Per al nostre cas utilitzarem les opcions de "Visible" i "Data net".

Configuració del PIRE dels equips escollits

En sistemes de Radiocomunicació, la Potencia Isotròpica Radiada Equivalent (PIRE) es la quantitat de potencia que emetrà una antena isotròpica teòrica, es a dir, aquella que distribueix la potencia exactament igual en totes les direccions, per a produir la densitat de potencia observada en la direcció de màxim guany d'una antena. El PIRE te en compte les pèrdues de la línia de transmissió i en els connectors i inclou el guany de la antena.

Aquest valor determinat PIRE (potencia isotròpica radiada equivalent), correspon a la relació: PIRE= potencia màxima transmesa + guany de la antena – pèrdues.

Coneixent el PIRE i el guany de la antena real es possible calcular la potencia real i els valors del camp electromagnètic. El PIRE s'utilitza per a estimar l'àrea en el que la antena pot donar servei i coordinar la radiació entre transmissors per a que no es solapin les cobertures.

La potencia total permesa en equips Wimax es de 21 dBm i de 20 dBm en Wifi, existint un valor de potencia màxim permès segons la legislació espanyola d'1 W per a Wimax i de 200 mW per a Wifi.

Procedirem al càlcul dels valors PIRE de la xarxa Wimax i Wifi utilitzant els equips escollits per als diferents veïnats del municipi, sempre seguint els valors proporcionats pel fabricant.

Taula de càlcul de potencia de transmissió màxima en funció del pire

Equip / Tecnologia	Potencia	Guany	PIRE màxim	Potencia
ARBA LINK 350	28 dBm	23 dBi	30 dBm (1W)	7 dBm
ARBA PRO-BS-1400	29 dBm	23 dBi	30 dBm (1W)	7 dBm
ARBA PRO-SU-1200	29 dBm	23 dBi	30 dBm (1W)	7 dBm
AP-24-8 Wifi	26 dBm	8 dBi	23 dBm (200	15 dBm

De tal manera que hem hagut de reajustar la potencia dels equips del radioenllaç, estació base i subscriptora a 7 dBm i els ap a 15 dBm, per tal d'ajustar-nos a la legislació.

El programa Radio Mobile te uns valors predeterminats per tal de calcular la qualitat de la senyal, essent *S0* un nivell de senyal baix i *S9+30* molt bona, en el nostre cas hem aconseguit senyals entre S9 i S9+30

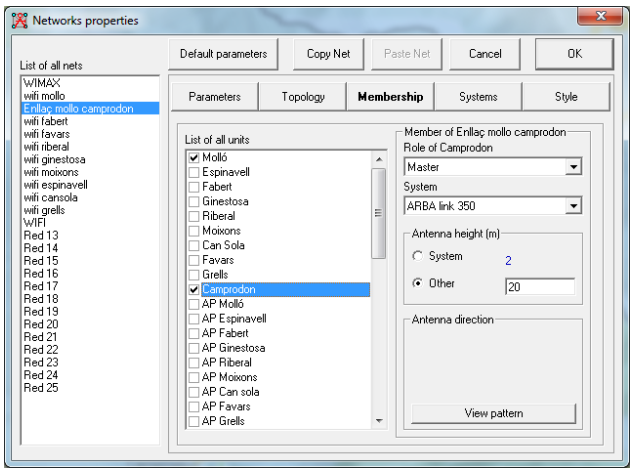
Taula de Marge respecte al Umbral de sensibilitat del receptor

Referencia codi S	Marge de fading (M) respecte al umbral
S0	M <= -1,5 dB
S1	-1,5 dB < M <= 1,5 dB
S2	1,5 dB < M <= 4,5 dB
S3	4,5 dB < M <= 7,5 dB
S4	7,5 dB < M <= 10,5 dB
S5	10,5 dB < M <= 13,5 dB
S6	13,5 dB < M <= 16,5 dB
S7	16,5 dB < M <= 19,5 dB
S8	19,5 dB < M <= 22,5 dB
S9	22,5 dB < M <= 27 dB
S9 + 10	27 dB < M <= 39 dB
S9 + 20	39 dB < M <= 49 dB
S9 + 30	49 dB < M <= 59 dB

Configuració del radio enllaç entre Camprodon i Molló

Primerament ens centrarem en la connexió a internet que arribarà a l'ajuntament a través d'una connexió amb un proveïdor de serveis d'internet o ISP. En el nostre cas el proveïdor escollit serà Movistar, la primera opció era intentar arribar directament amb fibra òptica però no es possible, nomes podem accedir amb adsl de baixa velocitat des de la central que es troba a Camprodon (8 kilòmetres de distancia). Com que volem garantir una velocitat de connexió de 256 Kbps com a màxim per a usuari, hem de contractar un radioenllaç de 125 Mbps des de Camprodon a Molló.
Un cop incorporats totes les configuracions globals, hem de configurar el tipus d'equips i antena que utilitzarem. Dintre de *Networks properties – Membership*

Pertinència a la xarxa de la estació de referencia i rol Master.



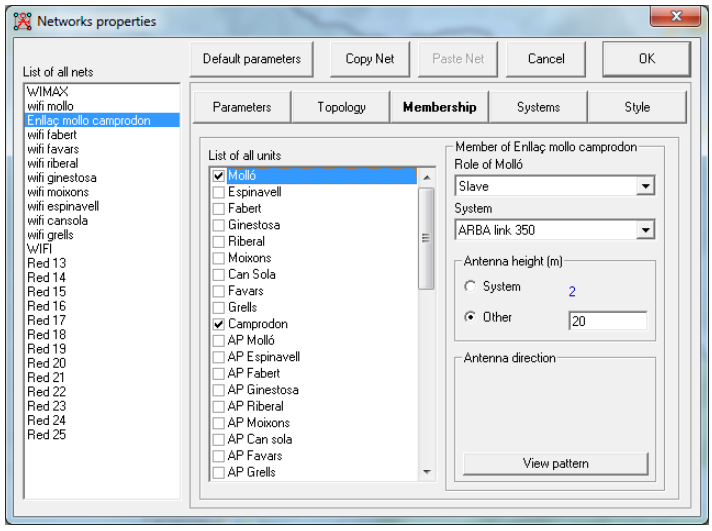
Seleccionem la xarxa de treball en el marc de l'esquerra (Enllaç Molló Camprodon). A continuació, en el marc *List of all units* marquem la estació de referencia y configurem els següents paràmetres:

- **"Role of …"**: com estam en una xarxa de tipus Data *net*, seleccionen *Master* per a la estació de referencia.
- **"System"**: escollim el model dintre dels disponibles en el llistat desplegable.
  A l'exemple el model del fabricant ARBA link 350
- **"Antenna height (m)"**: alçada de la antena des de el sol a l'emplaçament.

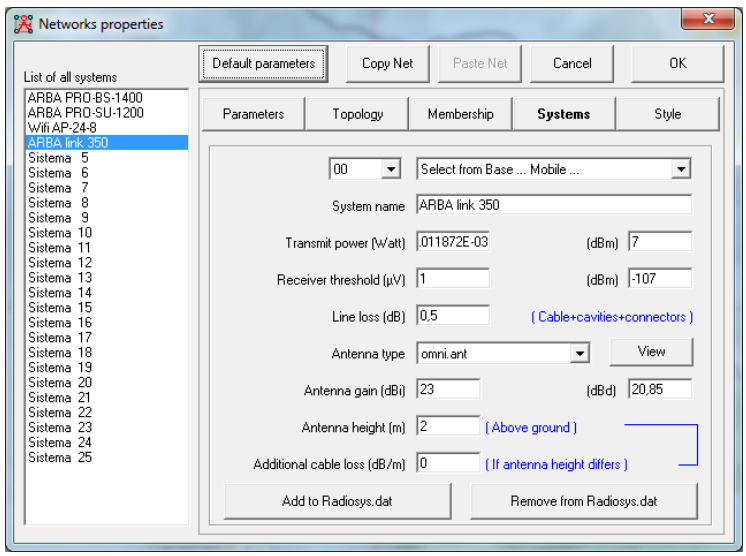
Al nostre exemple la alçada de les antenes del repetidor es de 20 metres per sobre del sòl.

A continuació, repetirem les mateixes passes per a la **estació subscriptora**, tenint en compte d'escollir *Slave* en el camp **"Role of…"**.

Pertinència a la xarxa de la estació de referencia i rol Slave



Un cop indicats el tipus d'equips i antena que utilitzarem, dintre de *Networks properties – Systems*

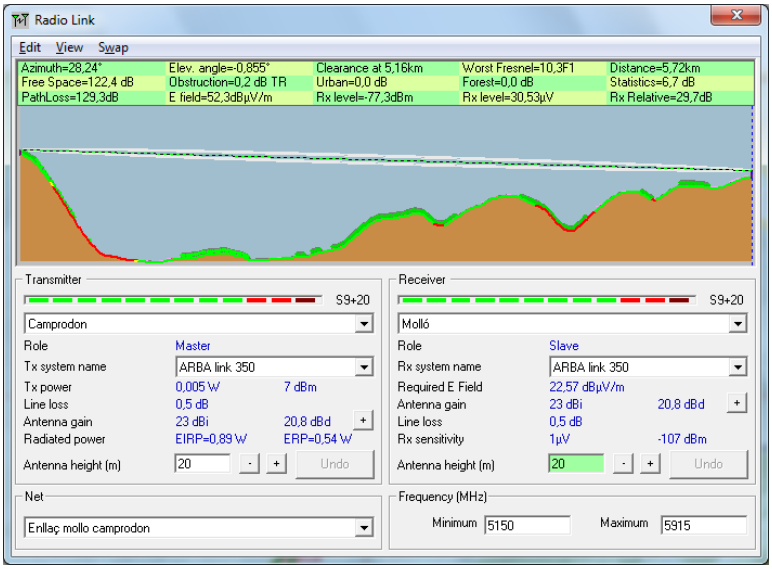


Seguidament omplirem la fitxa en el sistema, amb les dades que hem consultat en els manuals tècnics inclosos en la web del fabricant.

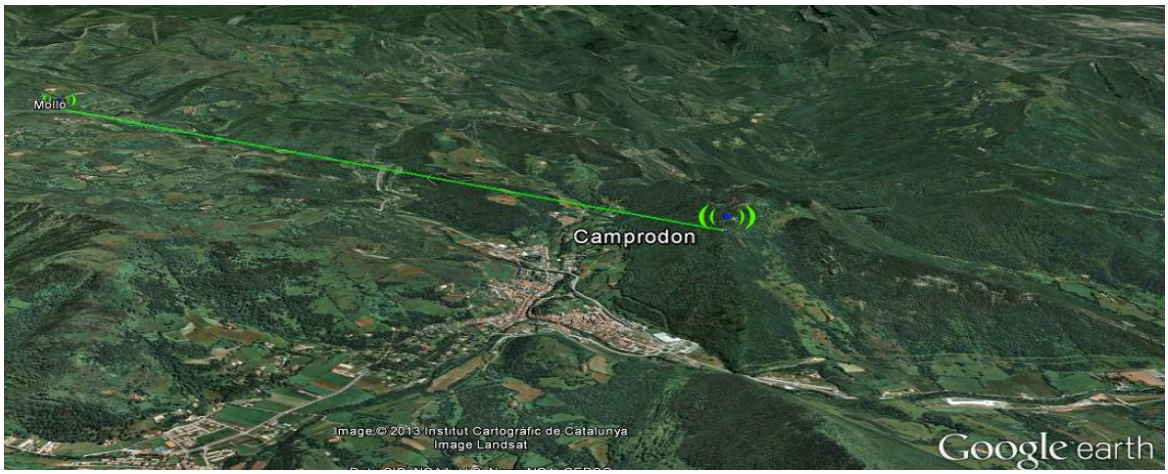
El primer pas es, per tant, seleccionar un registre lliure en el marc esquerre i assignar-li un nom en el camp *System name*. Per a cada equip que es registri, hem de definir els següents paràmetres:

- *"Transmitter power (Watt/dBm)":* potencia de transmissió en watts o en dBm. Nomes es necessari omplir un dels dos camps, ja que el programa calcula automàticament l'altre. Al nostre exemple la potencia transmesa es de 7 dBm.
- *"Receiver threshold (µV / dBm)":* sensibilitat del receptor en microvolts o en dBm. Nomes es necessari omplir un dels dos camps, ja que el programa calcula automàticament l'altre. Al nostre exemple la potencia transmesa es de -107 dBm.
- *"Antenna gain (dBi / dBd)":* guany de la antena referida a la de la antena isotròpica (dBi) o a la del dipol de mitja longitud d'ona de treball (dBd). Nomes es necessari omplir un dels dos camps, ja que el programa calcula automàticament l'altre. Al nostre exemple el guany de la antena es de 23 dBi.

Podem observar que a una distancia de 5,72 Km, segons les dades introduïdes, existint LOS, hi ha perfecta connectivitat entre ambdós equips. El valor de la senyal es de S9+20, que segons hem indicat anteriorment es molt alt.



Un cop tenim totes les dades generades, podem exportar-les a google earth i representar les dades d'una manera mes visual, veient les altituds del relleu en tres dimensions.



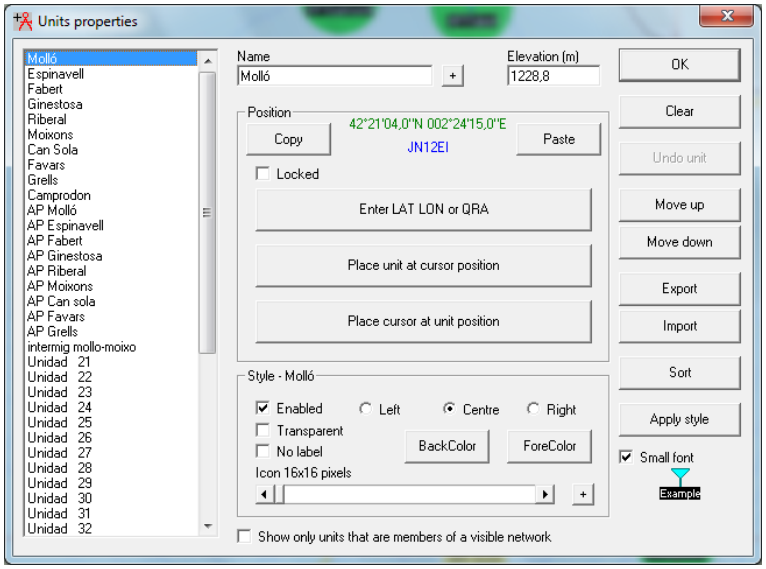
Configuració Wimax

El programa Radio Mobile es capaç de superposar un mapa topogràfic real amb les dades simulades del nostre radioenllaç, per aquest motiu tenint les diferents coordenades del municipi podem simular la cobertura de la xarxa dissenyada.

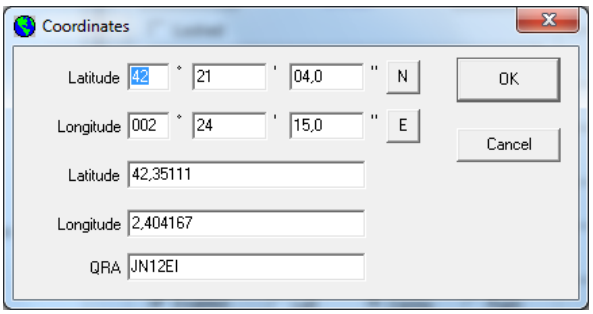
Coordenades reals de posicionament de les estacions als diferents veïnats

VEINAT	Coordenades de posicionament	
Molló	42,347 N	2,4048 E
Espinavell	42,378123 N	2,399247 E
Fabert	42,37699 N	2,4153 E
Ginestosa	42,35144 N	2,413216 E
El Riberal	42,348661 N	2,411445 E
Moixons	42,328966 N	2,44036 E
Can Solà	42,344502 N	2,404427 E
Favars	42,350171 N	2,391028 E
Grells	42,369230 N	2,395449 E
Punt intermig Molló-Moixons	42,33611 N	2,428611 E

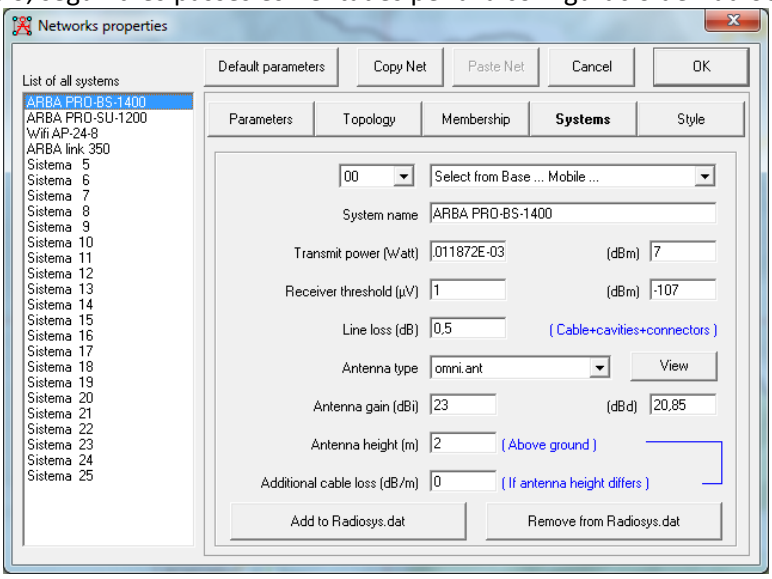
File i després *unit properties* es a on declararem les coordenades dels diferents membres de la xarxa indicades anteriorment.



Enter LAT LON or QRA i inserim les coordenades de latitud i longitud



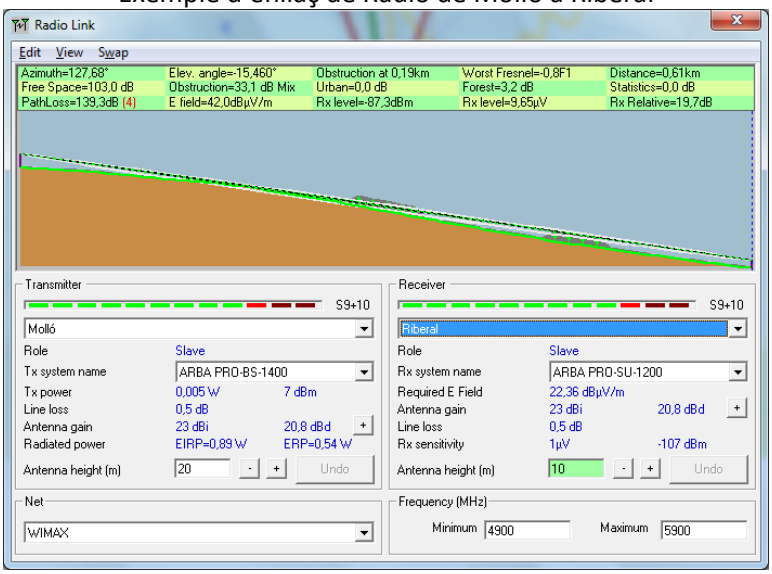
En aquesta captura podem veure la configuració de les unitats dels membres de la xarxa i la seva configuració, seguint les passes esmentades per a la configuració del radioenllaç.



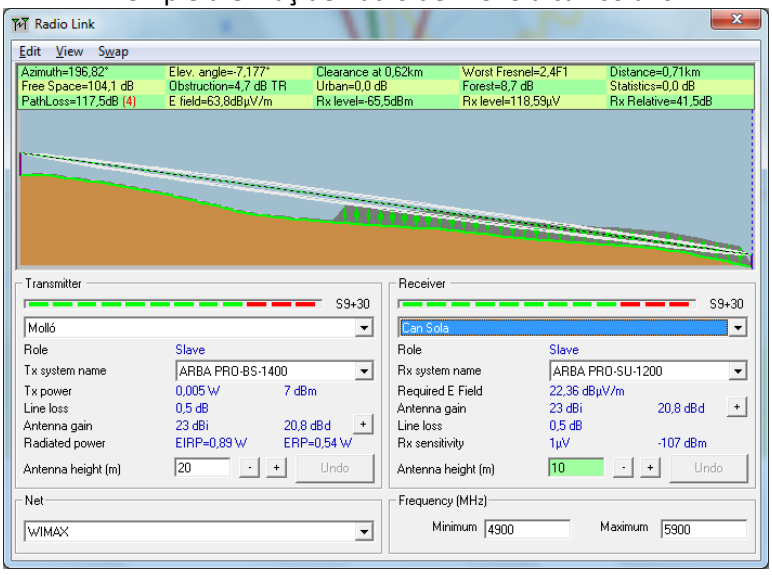
Un cop configurat tots els elements de la estació base i les unitats subscriptores hem posat com a estació base Molló, per tant el rol serà de Màster, i la resta de veïnats com a esclaus d'aquests, ja que son estacions subscriptores.

Un cop enllaçades totes les estacions base amb les unitats subscriptores podem representar la visibilitat de l'enllaç de radio de les mateixes. A continuació poso alguns exemples.

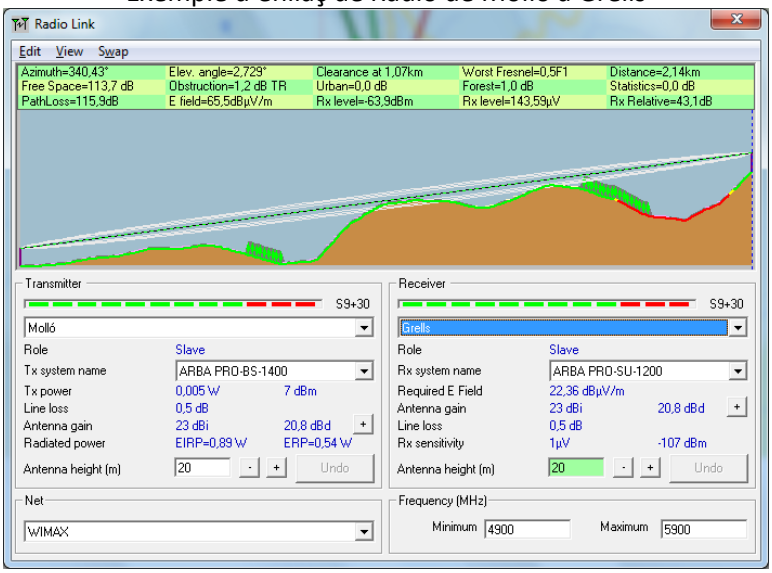
Exemple d'enllaç de Radio de Molló a Riberal



Exemple d’enllaç de Radio de Molló a can solans



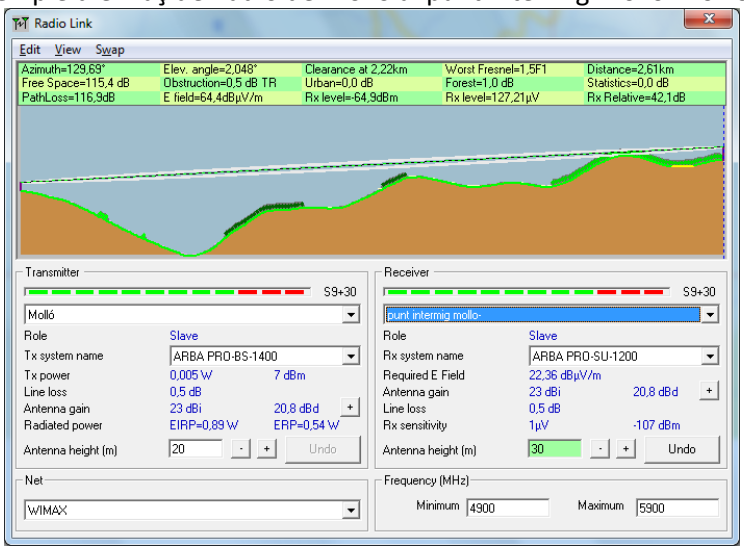
Exemple d’enllaç de Radio de Molló a Grells



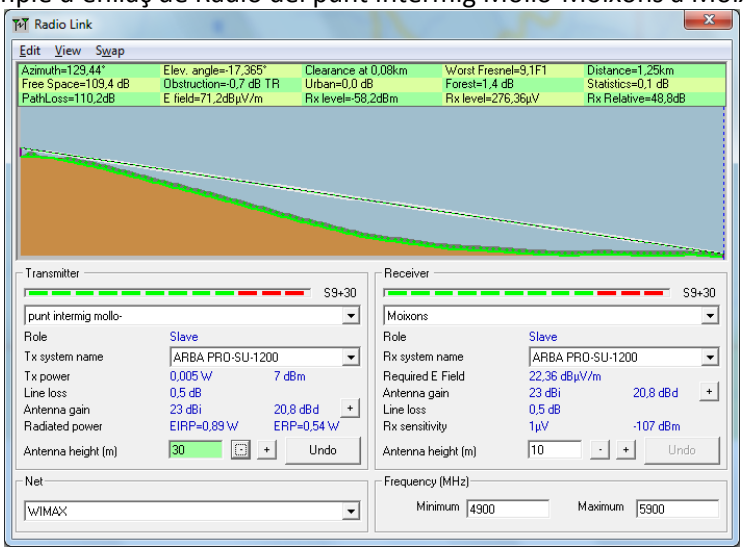
<u>Replantejament ubicació estació Molló - Moixons</u>

Ens trobem amb una circumstancia que no havíem previst inicialment. L’ orografia del terreny fan difícil la visibilitat entre ambdós punts plantejats inicialment de manera directa, i hem hagut de plantejar una nova solució posant un nou equip entre mig dels dos veïnats, per tal de fer arribar la senyal en bones condicions.

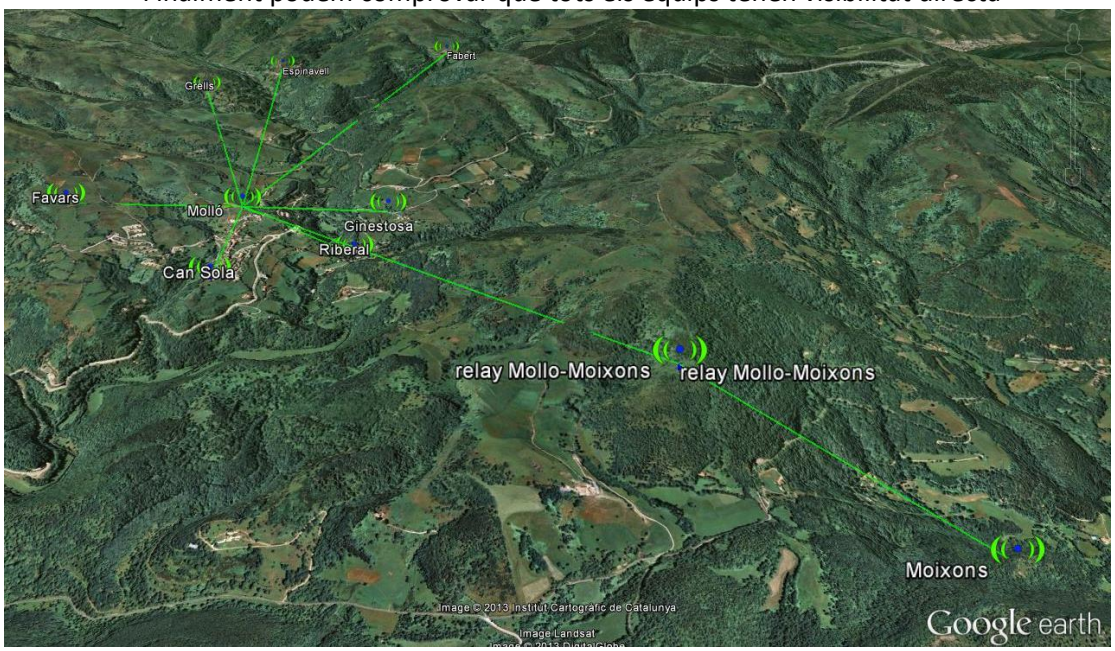
Exemple d’enllaç de Radio de Molló al punt intermig Molló-Moixons



Exemple d’enllaç de Radio del punt intermig Molló-Moixons a Moixons



Finalment podem comprovar que tots els equips tenen visibilitat directa



Configuració Wifi

La instal·lació dels punts d'accés dels diferents veïnats nomes requeriran d'una connexió de font d'alimentació que esta regulada, estabilitzada i protegida contra curtcircuits o canvis de polaritat, que proporciona el mateix fabricant integrat a l'equip escollit.

Els punts d'accés a la xarxa de cada veïnat tindrà el mateix nom que el SSID amb un guio i una lletra W indicant que es un equip que dona servei wifi, i un numero diferenciador de quantitat.

Identificació dels punt d'accés de cada veïnat

Punt d'accés wifi Molló – MOLLO-W1,
Punt d'accés wifi Espinavell – ESPINAVELL-W1
Punt d'accés wifi Fabert – FABERT-W1
Punt d'accés wifi Ginestosa – GINESTOSA-W1
Punt d'accés wifi El Riberal – ELRIBERAL-W1
Punt d'accés wifi Moixons – MOIXONS-W1
Punt d'accés wifi Can Solà – CANSOLA-W1
Punt d'accés wifi Favars – FAVARS-W1
Punt d'accés wifi Grells – GRELLS -W1

La connexió Wifi estarà limitada per a usuari a 256 Kbps de baixada per aquest motiu cada VLAN tindrà una limitació de 12.5 Mbps, exceptuant la VLAN situada a Molló que aquesta tindrà una limitació de 25 Mbps. De tal manera que a mode de resum i per clarificar, repartirem l'ample de banda de la següent manera:

$$12.5Mbps * 8\ Veinats\ colindants = 100 + 25Mbps\ per\ l'ajuntament\ de\ Molló$$

Això està fet així perquè el servei Wifi en els carrers del poble es per poc més que navegar i veure el correu. Les connexions tipus peer to peer (p2p), streaming o protocols livestream, o qualsevol altre protocol que tingui un gran ample de banda, estaran bloquejades.

La configuració de les adreces de xarxa en el nostre cas estarà dividida en 9 VLANs [6], que seran cadascuna de les xarxes wifi dels veïnats que dotarem de servei.

Taula d'assignació de Vlans als diferents veïnats

Vlan	VEINAT	XARXA	RANG IP	MASCARA
2	Molló	192.168.2.0	192.168.2.1 / 192.168.2.254	255.255.255.0
3	Espinavell	192.168.3.0	192.168.3.1 / 192.168.3.254	255.255.255.0
4	Fabert	192.168.4.0	192.168.4.1 / 192.168.4.254	255.255.255.0
5	Ginestosa	192.168.5.0	192.168.5.1 / 192.168.5.254	255.255.255.0
6	El Riberal	192.168.6.0	192.168.6.1 / 192.168.6.254	255.255.255.0
7	Moixons	192.168.7.0	192.168.7.1 / 192.168.7.254	255.255.255.0
8	Can Solà	192.168.8.0	192.168.8.1 / 192.168.8.254	255.255.255.0
9	Favars	192.168.9.0	192.168.9.1 / 192.168.9.254	255.255.255.0
10	Grells	192.168.10.0	192.168.10.1 / 192.168.10.254	255.255.255.0

6 A la bibliografia podem trobar informació de com donar d'alta les vlans al switch catalyst

Les adreces IP les assignarem de manera automàtica per DHCP (Dynamic Host Configuration Protocol) depenent del AP on s'accedeixi.
A cada veïnat hi haurà un AP que tindrà un SSID amb el nom propi del veïnat per tal que sigui un identificatiu, de tal manera que els usuaris que hagin de connectar-se a la wifi ho puguin fer de la manera mes fàcil, rapida i còmoda possible.

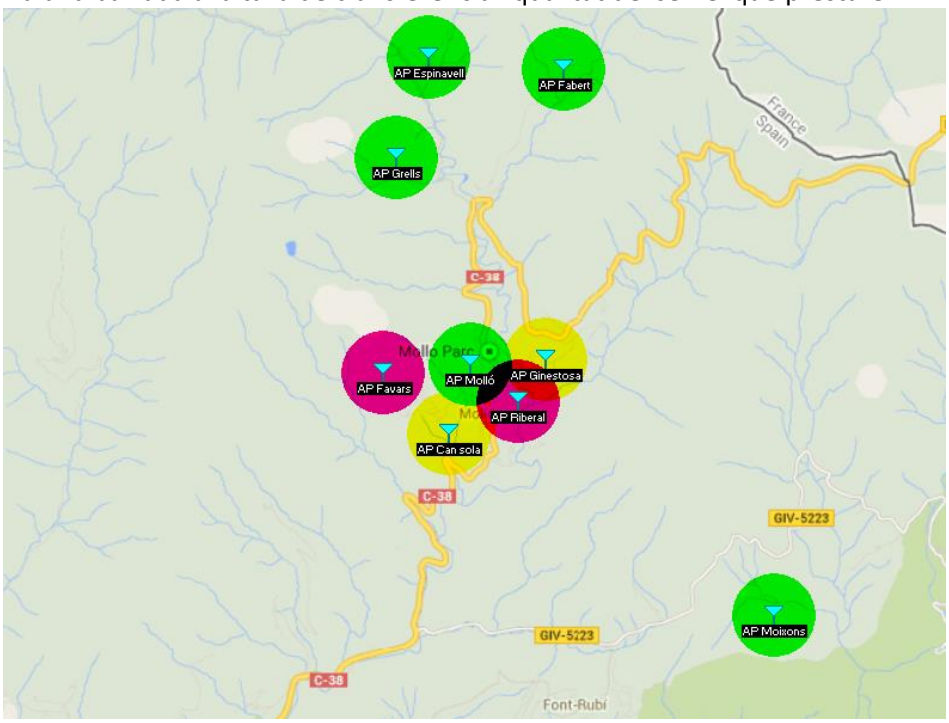
Identificació dels SSID de cada veïnat

CPE Molló	-	SSID: MOLLO
CPE Espinavell	-	SSID: ESPINAVELL
CPE Fabert	-	SSID: FABERT
CPE Ginestosa	-	SSID: GINESTOSA
CPE El Riberal	-	SSID: ELRIBERAL
CPE Moixons	-	SSID: MOIXONS
CPE Can Solà	-	SSID: CANSOLA
CPE Favars	-	SSID: FAVARS
CPE Grells	-	SSID: GRELLS

Utilitzant altre vegada l'eina de càlcul de cobertura, en la opció *Polar Radio Coverage*, podrem apreciar l'amplia cobertura dels punts d'accés Wifi ubicats al mateix mastil i per tant ubicació, que les estacions base i subscriptores dels enllaços Wimax.

Hem de destacar la superposició d'espectres dels Ap's, de tal manera que hem treballat amb els diferents canals que ofereix aquesta tecnologia per tal de donar una solució optima.
L'estàndard 802.11, te els següents canals útils: *Canal01: 2.412 Ghz*, Canal02: 2.417 Ghz, Canal03: 2.422Ghz, Canal04: 427Ghz, Canal05: 2.432 Ghz, *Canal06: 2.437 Ghz*, Canal07: 2.442 Ghz, Canal08: 2.447 Ghz, Canal09: 2.452 Ghz, Canal10: 2.457 Ghz,Canal11: 2.462 Ghz.

Tenim 3 canals no interferents (el 1 (Color Verd), 6 (Color Groc) i 11 (Color Rosa)).
Seran canals no interferents dos canals qualsevol que estiguin separats 5 canals (25MHz) entre sí. Això d'escollir Canals interferents es important, doncs si dos estacions estan transmetin en freqüències amb solapació, provocaran col·lisions i interferències entre si, hi aquest fet provocaria una baixada a la taxa de transferència i qualitat del servei que prestarem.



A continuació mostrarem un captura de com es veuria la publicació del SSID des de un dispositiu mòbil per tal de seleccionar una nova connexió de xarxa.

Immediatament després de fer la associació amb el SSID, ens apareixerà una pagina web de benvinguda, portal cautiu [7], en la qual podrem gaudir d'una navegació limitada en temps de 30 minuts amb una velocitat màxima de 256 kbps en cas de no ser soci o pel contrari, poder contractar altres modalitats en les que varia el temps del que podem gaudir d'una velocitat de fins a 6 Mbps, aquestes quotes són les seguents:

1 any: 42,00 € Soci anual
1 mes: 10,00 € Soci temporal
1 setmana: 6,00 € Soci col·laborador
1 dia (24h): 3,00 € Soci simpatitzant
15 minuts: 0,10 cents Soci passavolant

Tota aquesta gestió d'usuaris estara administrada pel servidor Radius, que ens proporcionarà seguretat al medi d'accés. A continuació mostrarem un captura de la redirecció a la pagina web d'autenticació.

7 A la bibliografia podem trobar informació detallada de com configurar un hotspot

Seguretat en xarxes Wifi

La seguretat en qualsevol xarxa inhalàmbrica ha de garantir bàsicament tres conceptes:

- Integritat : característica que garanteix que un missatge NO s'ha vist alterat en el camí des de l'emissor al receptor.
- Fiabilitat: garanteix que la informació només ha estat disponible per al destinatari autoritzat.
- Autenticació: amb el que es garanteix l'origen de la informació.

Amb l'objectiu de protegir les comunicacions sense fils, i conscients que la única forma de protegir-les és mitjançant l'ús de criptografia, han anat sorgint diferents protocols criptogràfics: WEP , WPA i WPA2.
Aquests dos últims, es diferencien en poc, ja que WPA va ser creat per ser no més que una transició a WPA2 mentre es completava el estàndard. L'estàndard contempla una sèrie de mesures bàsiques destinades a la protecció :

- Filtrat d'adreces MAC: Possibilitat de definir llistes de control d'accés, ACL (Access Control List), en els punts d'accés. Cadascun d'aquests punts pot comptar amb una relació de les adreces MAC de cada un dels clients que volem que es connectin a la nostra xarxa sense fil. Cada estació disposa d'una adreça que la identifica de manera inequívoca, i si el punt d'accés no la té donada d'alta, simplement no rebrà contestació per part seva.
  Cal tenir en compte que aquest no és el mètode més segur per protegir la entrada a la xarxa inhalàmbrica. Hi haurà d'actualitzar aquesta ACL cada vegada que es d'alta un nou client sense fil, eliminant aquells que volen deixar d'utilitzar.
- WEP (Wired Equivalent Privacy): El xifrat de la informació és una de les tècniques més utilitzades. És un sistema que genera una clau que es comparteix entre el client (STA) i el punt d'accés (AP), i que permet o denega la comunicació entre tots dos dispositius. WEP utilitza un sistema amb una clau de 64 o 128 bits, que poden ser hexadecimals o ASCII, per la qual s'autentica l'accés i s'encripta la informació que es transmet entre els dos dispositius.
  La seva manera de funcionament es resumeix de la a continuació:
  L'usuari introdueix una clau secreta (invariable) i a partir d'aquesta clau secreta i un IV (Inicialization Vector) que varia al llarg de la comunicació (per a cada paquet), es genera la clau de xifrat . El IV és de 24 bits perquè la majoria dels productes implementen 64bitWEP amb 40 bits per a la clau secreta i 24 bits per al IV. D'aquesta manera , s'introdueix confidencialitat en la informació transmesa. per introduir integritat en les dades fem ús d'un CRC (Cíclic Redundancy Check), amb això comprovem si les dades han estat alterades. Aquesta operació es realitza abans de la encriptació. Finalment enviem la trama xifrada, on introduïm de manera clara el IV, per posteriorment procedir a la des encriptació un cop rebuda. La autentificació per part de destinació, serà possible, sempre que, es conegui la clau secreta.
- WPA/WPA2 (Wifi Protected Access): amb l'objecte de dotar de major control i seguretat a les xarxes sense fil Wifi Alliance crea WPA que substitueix WEP. WPA millora la forma de codificar les dades respecte a WEP, utilitzant TKIP (Temporal Key Integrity Protocol), al mateix temps que proporciona autenticació d'usuaris mitjançant 802.1xi EAP (Extensible Authentication Protocol).

En realitat la diferència més important entre ambdós (WPA i WPA2) és que WPA segueix implementant l'algorisme de xifrat RC4, i utilitza com a protocol de gestió de claus TKIP mentre que WAP2 implementa l'algorisme de xifrat AES (Advanced Encryption Standard) mes segur que RC4, donant lloc a un nou protocol de encriptació anomenat CCMP (Counter Mode with Cipher Block chaining Message Authentication Code Protocol).

Per minimitzar el perill que suposa la implementació d'una xarxa sense fils, hi ha una sèrie de normes bàsiques a tenir en compte a l'hora de configurar la xarxa, com ara:

• Canviar la configuració per defecte: En contra del que sol pensar-se, són molts els administradors de la xarxa que no canvien la configuració fixada en fàbrica. Paràmetres com les claus i usuaris o el nom de xarxa es mantenen inalterats. És cert que la en la majoria de les instal·lacions es canvia el nom de la xarxa, però una cosa tan important com la clau d'accés de l'administrador, en molts casos, es manté inalterada, provocant un punt d'accés simple per a qualsevol intrús.

• Activar encriptació: És una de les pràctiques claus i necessàries. És el mètode bàsic i més immediat d'impedir accessos no autoritzats a la xarxa, així com captures de trànsit i dades privades. Hi ha diversos sistemes d'encriptació que analitzarem en un punt posterior.

• Ús de claus " fortes": Ja que és la clau a la xarxa, les claus que han de ser suficientment segures i complexes d'esbrinar per assegurar la seguretat de la xarxa. És freqüent utilitzar claus de sol lletres, amb paraules comunes i molt habitualment referenciat a dades personals de l'administrador, com noms de fills, edats, etc. Que fan la clau fàcil d'esbrinar.

• Desactivar l'anunci del nom de xarxa (SSID) : Encara que no és viable en tots els casos , la desactivació de l'anunci del nom de la xarxa és un element de seguretat afegit . D'una banda, impedirà l'atacant identificar la naturalesa i propietari de la xarxa, i per un altre farà necessari introduir el nom de la xarxa a mà per permetre l'associació a la xarxa Wifi, de manera que prèviament haurà de ser coneguda per l'atacant.

• Filtrats d'adreces MAC: En la majoria dels punts d'accés és possible especifica una llista d'adreces MAC que seran admeses, sent totes les altres rebutjades. L'adreça MAC és una adreça de nivell 2 que porta la targeta de xarxa Wifi gravada de fàbrica (anàloga a l'adreça MAC-Ethernet. Per tant, si es permet només l'accés a les adreces MAC pertanyents als equips propis s'impedirà que algun sistema extern pugui connectar-se de forma accidental o premeditada. No obstant això, cal fer notar que hi ha targetes de xarxa que permeten el canvi de l'adreça MAC, i en aquest cas seria possible per un atacant de la nostra xarxa, assignar-li una adreça vàlida d'algun dels nostres equips i evitar aquesta mesura de seguretat. No obstant això per a això, l'atacant, hauria de conèixer l'adreça MAC d'algun dels nostres equips, la qual cosa si les mesures de seguretat física i informàtica estan correctament implementades no serà fàcil.

• Ús d'adreces IP estàtiques: No un problema real per a un hacker amb coneixements, pitjor si dificulta l'accés a intrusos ocasionals. És habitual tenir a les xarxes Wifi l'assignació automàtica d'adreces IP, Gateway i DNS. La pràctica d'assignar les adreces manualment als terminals sense fil té l'avantatge que l'atacant ha d'esbrinar en primer lloc les dades de la xarxa, i més

important, ens permet habilitar filtres de manera que només les adreces IP assignades siguin permeses. En cas que l'atacant utilitzi alguna de les IP assignades, eventualment podrà ser detectat ja entrarà en conflicte amb els terminals legals.

• VLAN pròpia per a la xarxa Wifi. És interessant la implementació, en aquells equips que ho permetin, d'una VLAN específica per a la xarxa Wifi. Com que és una xarxa insegura per la seva naturalesa, és recomanable mantenir separada en tot moment de la xarxa cablejada. Així doncs, si el punt d'accés, o el controlador associat, és capaç de gestionar VLANs, mantenir el trànsit provinent de la xarxa Wifi en una VLAN diferent permetrà implementar mecanismes de seguretat i accés suplementaris que controlin l'accés dels usuaris Wifi a les dades de la xarxa corporativa.

• Instal·lació d'un Firewall: Relacionat amb el punt anterior, l'accés dels clients Wifi a la xarxa cablejada hauria de ser gestionat per un Firewall, ja sigui actuant de pont entre les corresponents VLANs o com a element físic de control, interposant-se en flux de trànsit Wifi. En qualsevol arquitectura, la inclusió d'un tallafocs ens permetrà implementar polítiques d'accés segures i complexes que assegurin que, encara que algun intrús hagués aconseguit connectar-se a la xarxa sense fils, no progressi fins a tenir accés a dades sensibles.

Aquestes mesures, per si mateixes, correctament implementades proporcionen seguretat suficient per a entorns no sensibles. No obstant això hi ha la possibilitat d'augmentar la seguretat mitjançant tècniques avançades, part de les quals necessiten de la participació d'un controlador de punts d'accés.

Configuració massiva d’equips

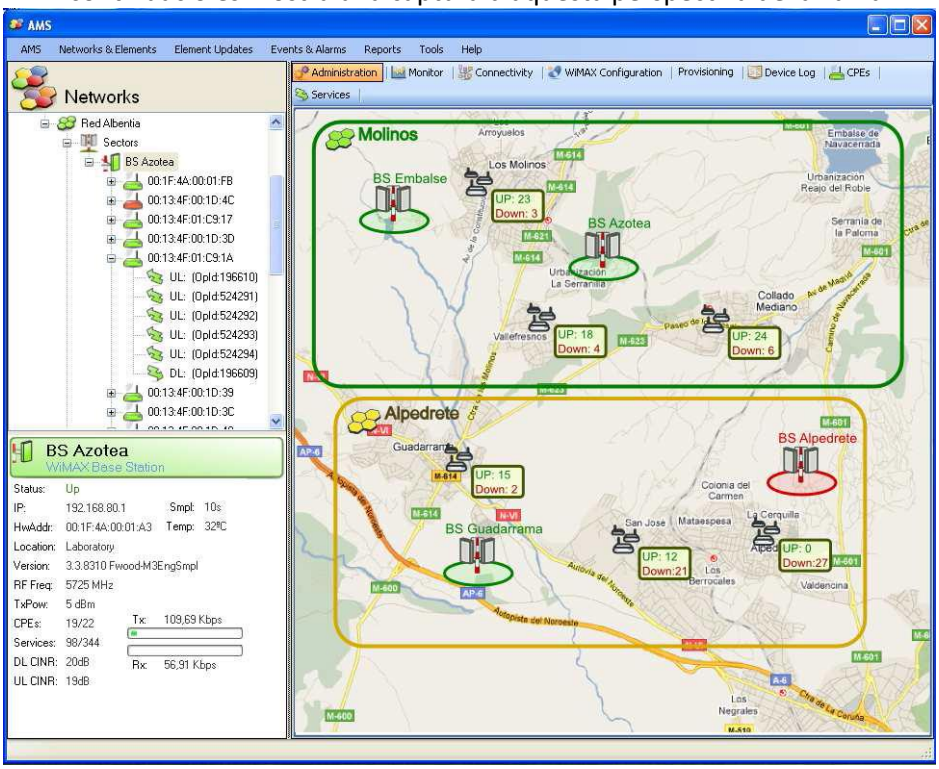
Un cop tenim instal·lats els equips als mastils i orientats, nomes ens quedarà configurar els equips amb els paràmetres esmentats anteriorment. De tal manera que podrem fer servir l’eina de configuració massiva d’equips proporcionada pel mateix fabricant.

AMS proporciona un altre utilitat per a la configuració d’equips que consisteix en efectuar el mateix canvi en diversos equips a la vegada. Això ajudarà molt al operador de la xarxa en el moment del desplegament, ja que es tracta de replicar configuracions de tot o part del sistema de xarxa.

AMS Selecciona una sèrie de paràmetres no crítics per canviar en bloc com poden ser paràmetres administratius o paràmetres ràdio com ara canal , prefix cíclic , limitació de modulacions, entre d’altres. Així l' usuari del AMS indicarà l'abast del canvi i aquest es realitzarà en bloc estalviant a l'administrador de xarxa temps i molèsties .

Com a eina indispensable per a la configuració massiva d'elements , aquest mòdul afegeix a les vistes bàsiques, un control per a visualitzar la topologia geogràfica de la xarxa . Juntament amb l'arbre d'elements, que proporciona la topologia lògica de la xarxa , aquestes dues eines permeten visualitzar el desplegament de xarxa i així organitzar canvis massius en la configuració tenint en compte petites interrupcions en el servei que puguin donar lloc a disminució momentània de la cobertura ràdio.

A continuació es mostra una captura d'aquesta perspectiva de la xarxa :



En cada equip Wimax prèviament i per que tingui visibilitat l'eina de monitorització, haurem de configurar la adreça IP, la freqüència de treball, canals i potencia de transmissió màxima.

En els diferents punts d'accés haurem d'accedir prèviament mitjançant la xarxa d'àrea local o wifi del mateix equip, des de un terminal extern i configurar el mode d'operació, en el nostre cas (b/g/n), indicar el guany de la antena i la potencia de sortida tenint en compte els càlculs anteriors del PIRE. Configurar la adreça IP a través de la que es podrà realitzar la gestió remota. La resta de paràmetres un cop establerta la comunicació la podem configurar des de la utilitat de configuració AMS, tals com configurar els SSID dels equips, seguretat, configuració dels canals 1, 6 i 11 perquè els punts d'accés no tinguin solapament, la carrega màxima permesa i els accessos dels usuaris.

Pressupost

A continuació es desglosa el pressupost previst global referent a l'execució dels treballs i l'equipament necessari per al desenvolupament del projecte.

Quantitat	Descripció	Concepte	PVP	Total
2	ARBA Link-350	Radioenllaç	900	1800
1	ARBA PRO-BS-1400	Estació Base	4800	4800
10	ARBA PRO-SU-1200	Estació subscriptora	1200	12000
1	AMS - AAS (as a Service)	Sistema gestió xarxa	900	900
1	Palo Alto PA-2050	Tallafocs	1900	1900
1	Cisco Catalyst 2960-48PST-L	concentrador	1200	1200
1	Dell PowerEdge R210 II	Servidor	1527	1527
1	connexió internet 125 Mbps simètrics	preu anual	2500/mes	30000
9	AP-24-8: 2.4GHz	Outdoor Acces Point	1527	13743
1	ma d'obra muntatge	ma d'obra muntatge	4000	4000
1	Servei de manteniment	manteniment	2000	2000
			Total	73870

Conclusions

En aquest projecte, hem analitzat la viabilitat de la implantació d'una xarxa sense fils al municipi de Molló. L'Ajuntament compte amb un pressupost anual de 464.255,29 euros[8], sent el nostre projecte d'una inversió de 74.000 euros i amortitzable en dos anys, podem prestar un servei interessant des del punt de vista del desenvolupament de la societat de la informació, i sense necessitat de realitzar obres que suposin un retard en la implantació d'aquest. En termes de temps la xarxa estaria operativa en 3 mesos, per donar servei als veïnats obtenint un rang de cobertura pràcticament total.

He tingut especial interès en trobar un fabricant per a la tecnologia WiMAX i WiFi que fos al màxim compatible amb altres marques, permetent en el futur una escalabilitat no lligada al fabricant, únicament al producte. En tractar-se d'una tecnologia madura, el cost d'implantació és raonable per al benefici que se n'obté.

La decisió de convivència d'ambdues tecnologies, Wimax i Wifi ha estat provocada, amb la intenció de permetre l'accés al major nombre d'usuaris possibles. Qualsevol terminal mòbil compta actualment amb suport WiFi i la utilització de WiMAX ens permet un desplegament de la xarxa troncal més econòmic i ràpid.

En un municipi orientat a serveis, on el turisme és una activitat econòmica que gaudeix de gran entitat, el poder oferir una connexió gratuïta serà un plus a oferir com a mostra de la seva modernitat.

Encara que per tal de garantir la viabilitat econòmica i d'amortització, tenint en compte el retorn de la inversió , he posat especial interès a la captació de clients, en el nostre cas anomenats socis, intentant sempre que siguin ofertes competitives i assequibles econòmicament.

El fet de voler prestar el servei de manera gratuïta, ha suposat l'obligació de realitzar limitacions en la velocitat del servei per tal de no alterar la competència al mercat i produir una competència deslleial. Tot i això, comptarem amb una velocitat raonable de 256 kbps pels no socis amb una duració per usuari i dia de trenta minuts i que permetrà la utilització dels serveis més comuns.

Respecte a la situació dels equips sempre s'ha intentat minimitzar la infraestructura a instal·lar, intentant en tot moment conviure amb elements ja existents, i en cas de nova instal·lació evitar la visió directa des del carrer, permetent reduir l'impacte visual i urbanístic.

Amb el disseny i instal·lacions de l'equipament planificat durant la realització del projecte s'acompleixen les propostes i justificacions definides inicialment al projecte. A més a més amb la simulació realitzada amb l'aplicació Radio Mobile es disposa de la viabilitat tècnica de la solució proposada. Encara que he pogut veure com sovint l'estudi i la realització del projecte

8 http://media.wix.com/ugd/1745ef_0e6af197f89d49379b8eb2eabdd304bc.pdf

es poden veure modificats per la realitat, com al radioenllaç entre Molló i Moixons, que hem hagut de posar un punt intermig per tal de tenir visió entre ambdós punts a causa de l'orografia del terreny.

S'ha definit una xarxa de telecomunicacions pròpia des de l'Ajuntament que ofereix connectivitat a 9 veïnats del municipi, permetent gaudir a la gent del poble i als visitants d'una una xarxa de comunicacions sense fil que ofereix el servei d'accés a Internet als habitants de la població i donant cobertura a totes les zones planificades inicialment, respectant al màxim l'arquitectura paisajistica i les infrastures ja existents a l'hora d'instal·lar nous elements.

Escalabilitat

Sempre hem disposat d'una capacitat de transport lliure dintre de la nostra xarxa troncal per realitzar una ampliació de la xarxa per interconnectar mes punts Wimax o ampliar nous punts d'accés Wifi per donar cobertura a nous punts de la població.

Bibliografia

Llei General de les telecomunicacions

https://www.boe.es/buscar/doc.php?id=BOE-A-2003-20253

Asociación WIFI-Alliance

http://www.wi-fi.org/

wimax

http://es.wikipedia.org/wiki/IEEE_802.16

Enciclopèdia lliure de google

http://www.wikipedia.org/

Documentació referent a propagació

www.telfneco.uy/propapagacion-ondas.pdf

www.ecrm.com/clase-4/propagacion.pdf

www.propagationmodel.com

productes wimax de la companyia Albentia

http://www.albentia.com/

AMS Advanced Management System (AMS)

http://www.albentia.com/Docs/Datasheet%20AMS_Jul2011%20ESP.pdf

http://www.albentia.com/Docs/AMS-ProductBrochure-ES_Jul2011.pdf

Central Provisioning System

http://www.albentia.com/Docs/CPS-ProductBrochure-ES.pdf

Documentació relativa a la estació base i subscriptora

http://www.albentia.com/Docs/ARBA%20Link%20-%20Catalogo%20de%20producto.pdf

Antena outdoor accés point

http://www.albentia.com/Docs/AP-24-8_Datasheet-Jan12.pdf

Annex

Componentes del sistema

Estaciones Base ARBA AXS-BS-556 / 558 / 133 / 135 / 150

Disponibles en diferentes bandas de frecuencia (5.4 GHz, 5.8 GHz, banda completa de 5 GHz y 3.3-3.6 GHz), las estaciones base proporcionan cobertura a las redes de acceso y tienen capacidad para más de 200 CPEs por sector. Proporcionan hasta 35 Mbps netos (50 Mbps brutos) por cada canal de 10 MHz, y 140 Mbps netos agrupando cuatro sectores. También soportan canalización de 3.5 MHz, 5 MHz y 7 MHz.

Terminales de usuario ARBA AXS-CPE-130 / 150 / 230 / 250 / 500

Albentia Systems ofrece una gama de CPEs que permite cubrir todas las necesidades de despliegue en redes de acceso inalámbrico. Los equipos AXS-CPE-100/200 son CPEs de uso residencial de bajo coste y fácil instalación. El modelo CPE-500 está diseñado para cubrir los exigentes requerimientos de los usuarios *premium* y corporativos en aspectos mecánicos, ambientales y de capacidad. Toda la gama de CPEs está disponible con antena directiva integrada de diversas ganancias (desde 15 a 24 dBi) o conector N para antena externa y en varias bandas de frecuencias (3.3-3.6 GHz, y la banda completa de 5 GHz).

Repetidores para la extensión de cobertura RPT-56 y RPT-58

Los repetidores son un elemento fundamental en el despliegue de redes de acceso, ya que extienden la zona de cobertura de las estaciones base. Permiten aumentar el número de clientes potenciales de forma transparente y sin comprometer la inversión, la calidad de servicio o la latencia de la red. Están disponibles en la banda de 5 GHz, con doble conector N, alimentación PoE y el mismo formato compacto que las estaciones base ARBA Access.

Unidades de sincronismo SCU-4S

La unidad de interior SCU-4S permite agrupar estaciones base ARBA Access para formar una estación base multisector. La SCU-4S genera señales de referencia que permiten sincronizar las tramas TDD de las estaciones base para evitar las interferencias intersector. Para ello emplea una referencia interna u opcionalmente un GPS externo. Además, la unidad SCU-4S proporciona la alimentación PoE para las estaciones base, permite la gestión remota de esta alimentación y la configuración en modos redundantes.

Sistema de provisión centralizada CPS

En redes con múltiples estaciones base en las que se proporciona servicio a centenas o miles de clientes, la provisión distribuida integrada en las estaciones base ARBA Access se puede optimizar mediante el sistema CPS (*Central Provisioning System*). Esta herramienta proporciona una base de datos centralizada y replicable, a la que las estaciones base consultan las peticiones de acceso de los clientes así como los servicios que tienen contratados.

Sistema de gestión de red AMS

La herramienta AMS (Advanced Management System) es un sistema de gestión de red avanzado para solucionar las necesidades de operación y mantenimiento de las redes de acceso y está adaptado a las particularidades de una red de acceso inalámbrico. Con funcionalidad Full FCAPS, permite al operador reducir sus costes de mantenimiento y operación.

Solución integral para el operador SIO

Diseñado para ser ajustado a las necesidades de cada operador, el SIO es un sistema de integración de negocio con las operaciones de red inalámbrica. Permite hacer una gestión de clientes y servicios comerciales: facturación, instalación de equipamiento, control de stock y gestión de incidencias.

ARBA access

Especificaciones técnicas

	Estaciones Base				CPEs			
Especificaciones radio	AXS-BS-556	AXS-BS-558	AXS-BS-150	AXS-BS-130	AXS-CPE-130	AXS-CPE-150	AXS-CPE-250	AXS-CPE-230
Banda de trabajo [MHz]	5470-5725	5725-5875	5150-5875	3300-3600	3300-3600	5150-5875		3300-3675
Capacidad neta agregada	35 Mbps			35 Mbps	35 Mbps			24,2 Mbps
Ancho de canal	10 MHz			10 MHz	10 MHz			7 MHz
Eficiencia espectral neta	3,5 bps/Hz			3,5 bps/Hz	3,5 bps/Hz			2,42 bps/Hz
Sensibilidad máx. modulación	-74 dBm							
Máx. potencia de transmisión	26 dBm	26 dBm	26 dBm	26 dBm	26 dBm		20 dBm	
Antena integrada	Conector N		Conector N o Sectorial 60/90/120º	Conector N	130: N/16 dBi	150: N/15/19 dBi	Conector N 16/20/24 dBi	Conector N, 17/20 dBi
Modulación	OFDM de 256 portadoras según sección 8.3 estándar IEEE 802.16-2012							
Mod. subportadora	Adaptativa BPSK, QPSK, 16QAM y 64QAM (siete niveles diferentes con combinación FEC) según estándar IEEE 802.16-2012							
FEC	Sí, Reed-Solomon concatenado con código convolucional, según IEEE 802.16-2012							
DFS	Sí							
Downlink/Uplink	Desde 90/10 hasta 15/85 en BS, y desde 100/0 hasta 0/100 en CPE							
Acceso al medio	TDMA síncrono con implementación hardware, según IEEE 802.16-2012							
Técnica duplexión	TDD (Time Domain Duplexing)							
Sincronismo TDD	Sí, para más de un sector requiere unidad SCU							

Calidad de servicio				
Control de QoS	Cinco niveles de QoS según IEEE 802.16-2012 (BE, nRTPS, eRTPS, RTPS, UGS). Colas independientes por usuario y servicio.			
Máx. CPEs por sector	Ilimitados	20	Ilimitados	N/A
Diferenciación de servicios L2	Dirección MAC origen/destino, EtherType, etiqueta VLAN			
Diferenciación de servicios L3	DSCP, ToS, dirección IP origen/destino, subred, tipo de protocolo			
Diferenciación de servicios L4	Puerto TCP o UDP origen/destino			

Networking		
Funcionalidad capa 2	Bridging 802.1, VLAN 802.1q	
Funcionalidad capa 3	Routing dinámico/estático, NAT, DHCP servidor/cliente	
Cifrado	AES256	AES128
Latencia	5 ms extremo a extremo. Jitter típico < 0.5 ms	
Certificados X.509	Sí	
Interfaz de datos	Ethernet 10/100 Base-T	

Características físicas			
Rango de temperatura	De –30 °C a +55 °C (ambiente, en operación)		
Alimentador PoE	Entrada 100-240 VAC 50/60 Hz — Salida 56 VDC (Opción Entrada DC 18-72 VDC)	Entrada 110-240 VAC 50/60 Hz — Salida 24 VDC (Opción entrada DC 10-24V)	
Consumo de potencia	< 18 W	< 4,5 W	< 7 W

Estándares	
Radio	ETSI EN 301 893 V1.5.1 (5GHz), ETSI EN 302 502 V1.2.1 (5.8GHz)
Entorno	ODU: protección (IP67) (AXS-CPE-130 y AXS-CPE-150: IP55), ETSI EN 60950-1: 2006 (seguridad). IDU: IEC 61000-4-2 (ESD), IEC 61000-4-5 (Surge)

albentia systems

Albentia Systems S.A.
C/ Margarita Salas, 22 - 28918 Leganés - Madrid (ESPAÑA)
Tel.: +34 91 440 0213
Fax: +34 91 327 4342
E-mail: sales@albentia.com

www.albentia.com

albentia Systems

AP-24-8: 2.4GHz Outdoor Access Point

IEEE 802.11b/g/n

Product Overview

Today's wireless market, more specifically the outdoor wireless market, continues to demand higher transmit power, greater dependability and advanced feature sets, all while keeping the client-side cost down. To that end, **ALBENTIA SYSTEMS** has released its latest line of customer premise equipment developed for the unlicensed 2.4GHz ISM band, the AP-24-8.

The AP-24-8 is an all-in-one cost-effective, weatherproof wireless device featuring high output power as well as all the essential features for both operating as an Acess Point or a CPE Client. This dual approach offers greater flexibility and reduced inventory stock as this unit can perform all that is required for establishing reliable wireless networks. The AP-24-8 is unique in that it includes an 8dBi directional antenna for any point-too-point connection needs and when more power or coverage is required you can bypass the integrated antenna and connect a higher gain antenna to its N-male type RF connector*.

Please contact a sales representative for more information on samples, promotional pricing and availability on the AP series or any other Albentia Systems wireless products.

**for antenna limits please check with the regulations in your area*

AP-24-8 at a Glance

Chipset	Atheros AR9285/AR7240
Transmit Power	26 dBm
Receive Sensitivity	-90 dBm @ 6 Mbps data rate
Antenna (Software selectable)	8 dBi Panel antenna
	N-male type antenna connector

IEEE	Radio	RoHS	Interface
IEEE 802.11b/g	Atheros	RoHS	ETHERNET

AP-24-8 Highlights

Key Features

- IEEE 802.11b/g/n compliant
- Up to 26dBm output power
- WPA / WPA2 wireless security
- RoHS compliant
- Adjustable output power
- Chipset: Atheros AR9002 Family
  - CPU: Atheros AR7240
  - RF: Atheros AR9285
- Atheros Align technology
- Software selectable RF output
  - Integrated 8dBi antenna
  - N type male connector

System Specifications

Radio Specification				
Chipset Solution	RF: Atheros AR9285 | CPU: AR7240 (400MHz)			
Antenna – Default configuration	8dBi integrated directional antenna (vertical pol.)			
External RF connector	N type male connector – switchable by software			
Antenna Configuration	1 * 1 (1 Tx, 1 Rx)			
Memory	**Flash**	**DDR**		
	8MB	32MB		
Modulation	OFDM: BPSK, QPSK, 16-QAM, 64-QAM / DSSS: DBPSK, DQPSK, CCK			
Available Data Rates (Mbps)	IEEE 802.11b – 11, 5.5, 2, 1			
	IEEE 802.11g – 54, 48, 36, 24, 18, 12, 9, 6			
	IEEE 802.11n (draft) – 135, 130, 121.5, 117, 108, 104, 81, 78, 65, 58.5, 54, 53, 40.5, 39, 27, 26, 19.5, 13.5, 13, 6.5, 6			
RF Frequency	**USA (FCC)**	**Europe (ETSI)**		
	2.412GHz – 2.462GHz (Channels 1-11)	2.412GHz – 2.472GHz (Channels 1-13)		
	IEEE 802.11gn HT40 ISM band			
	2.422Ghz – 2.452GHz (Channels 3-9)	2.422Ghz – 2.462GHz (Channels 3-11)		
Average RF Output Power (± 1.5dB)* **actual power may vary based on regulatory requirements*	802.11b	26 ± 1.5dBm		
	802.11g	6-24Mbps	26 ± 1.5dBm	
		36-48Mbps	25 ± 1.5dBm	
		54Mbps	24 ± 1.5dBm	
	802.11n	HT20	MCS 0-3	26 ± 1.5dBm
			MCS 4	25 ± 1.5dBm
			MCS 5	24 ± 1.5dBm
			MCS 6	23 ± 1.5dBm
			MCS 7	22 ± 1.5dBm
		HT40	MCS 0-3	26 ± 1.5dBm
			MCS 4	25 ± 1.5dBm
			MCS 5	23 ± 1.5dBm
			MCS 6	22 ± 1.5dBm
			MCS 7	21 ± 1.5dBm
Receiver Sensitivity	**802.11b**	**802.11g**	**802.11n**	
	1Mbps: ≤ -93dBm	54Mbps: ≤ -73dBm	HT20/MSC0 ≤88dBm	HT40/MSC0 ≤84dBm
Regulatory Compliance	FCC Part 15, CE EN300 328, EN301 489-1/17, EN60950			
Standards Compliance	IEEE 8802.11bgn, WiFi certificate			
Physical Specification				
Dimension	165mm(l)x60mm(w)x34mm(h)			
Weight	≤ 400g			
Enclosure	IP55 Plastic			
Electrical Specification				
Reset Button	Reset to factory default			
Power Requirements	12VDC @ 1 A (switching)			
PoE	Passive 12V PoE			
Power Consumption	≤ 900mA @ 12VDC			
LED Definition	Power: Green on – system on, Green off – system off, Amber blinking – Initializing			
	LAN: Off – no Ethernet, On – connection established, Blinking – sending, receiving			
	WLAN (AP Mode) Off – disabled, On – WLAN enabled, Blinking – WLAN activity			
	WLAN (Client Mode) All Off – WLAN disabled, Green blinking – good connection Yellow blinking – Acceptable quality, Red blinking – poor connection quality			

System Specifications

Environmental Specification	
Operating Temperature	-20℃ ~ 70℃
Storage Temperature	-30℃ ~ 80℃
Operating Humidity (non-condensing)	10 to 95 % RH
Green	RoHs Compliant

Firmware Specification			
Function		**Detail**	**Default setting**
Web Language		English	English
Firmware Upgrade Method		Web upgrade via Ethernet or Wireless port / TFTP upgrade via Etherent port	
Status		Information	
		Statistics for Wireless and Ethernet	
		Connection status	
System	Basic Settings	Device Name	APXXXXXX
		Country/Domain	USA FCC
		Time NTP	Disable
	IP Settings	IP Address assignment (DHCP/Manual)	DHCP / 192.168.1.1, DHCP is the default, however when server is not present the unit reverts to 192.168.1.1
	RADIUS	Accounting and Authentication	Disable
Wireless	Basic Wireless Settings	Operation mode (AP / CPE / Bridge / AP Repeater)	AP
		AP mode functions	
		1. SSID	Wireless
		2. Hide SSID (enable/disable)	Disable
		3. Channel select (1-11)	1
		4. Client limitations (0~32)	32
		5. Wireless client isolation (enable/disable)	Disable
		6. Tx flow control (1~2400*64Kbps)	1687
		Client mode functions	
		1. SSID	Any
		2. CPE with Multi-Client support	Enable
		3. Tx Flow control by AP (enable/disable)	Disable
		Wireless mode	802.11b/g/n
		Data Rate Selection 1-54Mbps & MCS0-7	Best
	Security Settings	• Open system • Shared Key (64/128/152-bits WEP) • 802.1X only • WPA • WPA2 • WPA-PSK(TKIP) • WPA2-PSK(AES)	Open System
	Access Control	Allow / Deny STA list STA Flow control for allowed stations	Disable

System Specifications

Firmware Specification			
Function		**Detail**	**Default setting**
System	Advanced Settings	Radio on / off	On
		• Allow / Deny Station list • Station Flow control for allowed stations Supports up to 32 stations	Disable
		WMM Regatta Mode (enable/disable)	Disable
		Output power control: Options (full, 50%, 25%, 12.5%, min)	Full
		Fragmentation Length (256~2346)	2346
		Beacon Interval (20 ~ 10000ms)	100
		RTS/CTS threshold (0~2346)	2346
		DTIM Interval (1-255)	255
Management	Password	Change Password	Password
	Remote Management	Embedded Web configuration management	Enable
		Telnet support (password-protected telnet access to internal configuration manager)	Enable
		SNMP management	Enable
		FTP	Enable
		SSH - Command Line Interface	
	Configuration	• Web backup and restore configuration • Reset to factory default • Reboot	
Tools	Event Log		
	Site Survey		

Internal antenna – Electrical Specification	
Antenna Shape	Patch Array
Diemnsions	L154.0 x W32.0 x T1.0 mm
Antenna Material	FR 4
RF Frequency Band	2.4~2.5 GHz
Power Handling	2 W
Impedance	50Ω
VSWR	Less than 2.0
Palarization	Linear (Vertical)
Antenna Gain	Peak Gain@2.45Ghz – **8.45dBi**
Antenna Directivity	4.7dB
HPBW_Horizontal	**113º**
HPBW_Vertical	**39º**
Front to Back Ratio	17.92 dB
Operating Temperature	-30ºC~ +80ºC

Maximum Gain Value Table (dBi)			
	2.4 GHz	**2.45 GHz**	**2.5 GHz**
H-Plane (XZ Plane)	7.56	8.04	8.08
E-Plane (YZ Plane)	7.82	8.45	7.82

Firewall Palo Alto PA-2050

Technical Specifications:

Model	PA-2020	PA-2050
Performance and Capacities Specifications		
Firewall throughput (App-ID enabled)	500 Mbps	1 Gbps
Threat prevention throughput	200 Mbps	500 Mbps
IPSec VPN throughput	200 Mbps	300 Mbps
New sessions per second	15,000	15,000
Max sessions	125,000	250,000
IPSec VPN tunnels/tunnel interfaces	1,000	2,000
GlobalProtect (SSL VPN) concurrent users	500	1,000
SSL decrypt sessions	1,000	1,000
SSL inbound certificates	25	25
Virtual routers	10	10
Virtual systems (base/max)	1/6	1/6
Security zones	40	40
Max. number of policies	2,500	5,000
Hardware Specifications		
I/O	(12) 10/100/1000 + (2) SFP optical gigabit	(16) 10/100/1000 + (4) SFP optical gigabit
Management I/O	(1) 10/100/1000 out-of-band management port, (1) RJ-45 console port	
Storage Capacity	160GB HDD	
Power supply (Avg/Max power consumption)	250W (105W/120W)	
Max BTU/HR	409	

Input Voltage (Input Frequency)	100-240VAC (50-60Hz)
Max Current Consumption	3A@100VAC
Mean Time Between Failure (MTBF)	7.3 years
Max Inrush Current	70A@230VAC; 35A@115VAC
Rack Mountable	1U, 19" standard rack
Dimensions	1.75"H x 17"D x 17"W
Weight (Stand alone device/as shipped)	15lbs/20lbs
Safety	UL, CUL, CB
EMI	FCC Class A, CE Class A, VCCI Class A, TUV
Certifications	FIPS 140 Level 2, Common Criteria EAL2, ICSA, UCAPL
Environment	
Operating temperature	32° to 122° F, 0° to 50° C
Non-operating temperature	-4° to 158° F, -20° to 70° C

Networking Specifications:

Interface Modes

- L2, L3, Tap, Virtual wire (transparent mode)

Routing

- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR): 5,000/2,500 (PA-2050), 2,500/2,500 (PA-2020)
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

High-Availability

- Active/Passive with no session synchronization
- Failure detection: Path monitoring, Interface

VLANS

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 2,048 (PA-2050), 1,024 (PA-2020)
- Aggregate interfaces (802.3ad)

NAT/PAT:

- Max NAT rules: 1,000
- Max NAT rules (DIPP): 200
- Dynamic IP and port pool: 254
- Dynamic IP pool: 16,234
- NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
- DIPP oversubscription (Unique destination IPs per source port and IP): 2
- NAT64

Virtual Wire

monitoring

Address Assignment

- Address assignment for device: DHCP Client/PPPoE/Static
- Address assignment for users: DHCP Server/DHCP Relay/Static

IPV6

- Features: L2, L3, Tap, Virtual Wire (transparent mode)
- Services: App-ID, User-ID, Content-ID, WildFire and SSL Decryption

- Max virtual wires: 1,024 (PA-2050), 512 (PA-2020)
- Interface types mapped to virtual wires: physical and subinterfaces

L2 Forwarding

- ARP table size/device: 2,500 (PA-2050), 1,000 (PA-2020)
- MAC table size/device: 2,500 (PA-2050), 1,000 (PA-2020)
- IPv6 neighbor table size: 1,000

Security Specifications:

Firewall

- Policy-based control over applications, users and content
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Decryption: SSL (inbound and outbound), SSH

Wildfire

- Identify and analyze targeted and unknown files for more than 100 malicious behaviors
- Generate and automatically deliver protection for newly discovered malware via signature updates
- Signature update delivery in less than 1 hour, integrated logging/reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day (Subscription Required)

File and Data Filtering

- File transfer: Bi-directional control over more than 60 unique file types
- Data transfer: Bi-directional control over unauthorized transfer of CC# and SSN
- Drive-by download protection

User Integration (User-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One and other LDAP-based directories
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML API to facilitate integration with non-standard user repositories

IPSEC VPN (Site-To-Site)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamic VPN tunnel creation (GlobalProtect)

Threat Prevention (Subscription Required)

- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

URL Filtering (Subscription Required)

- Pre-defined and custom URL categories
- Device cache for most recently accessed URLs
- URL category as part of match criteria for security policies
- Browse time information

Quality of Service (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking
- Physical interfaces supported for QoS: 4

SSL VPN/Remote Access (GlobalProtect)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third party client support: Apple iOS, Android 4.0 and greater, VPNC IPSec for Linux

Management, Reporting, Visibility Tools

- Integrated web interface, CLI or central management (Panorama)
- Multi-language user interface
- Syslog, Netflow v9 and SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter and export traffic, threat, WildFire, URL, and data filtering logs
- Fully customizable reporting

Número de catálogo / Descripción	Código del producto	Qty	SKU	
Base: PowerEdge R210 II Chassis, 2x3.5" Cabled HDDs, LED Diagnostics	509787	1	[210-35616]	
Procesador: Intel® Xeon® Processor E3-1280v2, 4C/8T, 3.60GHz, 8M Cache, 69W TDP, Turbo	703666	1	[213-16167]	146
Memoria: 8GB Memory (1x8GB) 1600Mhz Dual Ranked Low Volt UDIMM (speed is CPU dependent)	774965	1	[370-AAFL][370-AAGP]	3
Sistema operativo instalado de fábrica: Windows Server 2008 R2 SP1, Foundation Edition, English, Including Media	727817	1	[617-10368][618-10611]	285
Conectividad Raid: C11 2HD/4HD - RAID 1 with PERC H200, Requires SAS/SATA/SSD Drives	509830	1	[780-12731]	1009
Primera tarjeta controladora RAID o SCSI: PERC H200 RAID Controller	509847	1	[405-11874]	278
Primera unidad de disco duro: 500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Cabled)	256898	2	[400-17639]	1209
Activación de UEFI: UEFI BIOS Setting	634945	1	[223-10289]	1228
Powercord: 2M Rack Power Cord C13/C14 12A	204752	1	[450-12466]	207
Tarjetas de administración del servidor: Embedded Baseboard Management Controller	256923	1	[565-10165]	1314
Carcasa frontal: 1U Rack Bezel	257406	1	[350-10513]	669
Guías para montaje en rack: No Rack Rails Included	509807	1	[770-11315]	88
Dispositivos ópticos: 16X DVD+/-RW ROM Drive SATA with SATA Cable	509819	1	[429-15829]	16
Administración de sistemas: PE R210II Electronic System Documentation and OpenManage DVD	509843	1	[631-10774]	49
Documentos de envío: R210II EMEA1 Ship Docs No Power Cord (English/French/German/Spanish/Russian/Hebrew)	509790	1	[340-25162]	21
Referencia del paquete Gedis: SVR210IIa	691058	1	[203-14860]	22
Información sobre el pedido: PowerEdge Order - Spain	32385	1	[800-10501]	111
Garantía básica: 1Yr Basic Warranty - Next Business Day - Minimum Warranty	313707	1	[709-10510][709-10511]	29

Configuració Vlan en switch Cisco Catalyst

Configuración de VLAN en switches Catalyst que ejecutan CatOS
Creación de VLAN y puertos
Complete los pasos de esta sección para crear una VLAN.
Antes de que pueda crearla, el switch debe estar en modo de servidor VTP o en modo transparente VTP. Si el switch es un servidor VTP, debe
definir un nombre de dominio VTP antes de agregar cualquier VLAN.
1. Defina un nombre de dominio VTP.
Debe definir el nombre de dominio VTP independientemente de:
El número de switches de la red, ya sea uno o varios
Si utiliza VTP para propagar las VLAN a los demás switches de la red
La configuración VTP predeterminada en el switch es la siguiente:
CatosSwitch> (enable)show vtp domain
Domain Name Domain Index VTP Version Local Mode Password
-------------------------------- ------------ ----------- ----------- ----------
1 2 server -
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
5 1023 0 disabled
Last Updater V2 Mode Pruning PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0 disabled disabled 2-1000
Ejecute el comando set vtp para establecer el modo y el nombre del dominio.
CatosSwitch> (enable)set vtp domain ?
<name> Domain name
CatosSwitch> (enable)set vtp domain cisco ?
mode Set VTP mode
passwd Set VTP password
pruning Set VTP pruning
v2 Set VTP version 2
CatosSwitch> (enable)set vtp domain cisco mode ?
client VTP client mode server VTP server mode
transparent VTP transparent mode
CatosSwitch> (enable)set vtp domain cisco mode server
VTP domain cisco modified
Nota: consulte Understanding and Configuring VLAN Trunk Protocol (VTP) (Introducción y configuración del protocolo de troncal
VLAN) para obtener más información sobre VTP.
2. Ejecute el comando show vtp domain para verificar la configuración VTP.
CatosSwitch> (enable)show vtp domain
Domain Name Domain Index VTP Version Local Mode Password
-------------------------------- ------------ ----------- ----------- ----------
cisco 1 2 server -
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
5 1023 1 disabled
Last Updater V2 Mode Pruning PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0 disabled disabled 2-1000

Nota: si tiene el resultado de un comando show vtp domain de su dispositivo Cisco, puede utilizar la herramienta intérprete de resultados
(sólo para clientes registrados) (OIT) para que se muestren los problemas potenciales y sus soluciones.
3. Después de configurar y verificar el dominio VTP, puede empezar a crear las VLAN en el switch.
De forma predeterminada, hay sólo una VLAN para todos los puertos. Esta VLAN se denomina default. No es posible eliminar ni
cambiar el nombre de VLAN 1.
Puede usar el comando show vlan para visualizar los parámetros de todas las VLAN configuradas en el dominio administrativo.
CatosSwitch> (enable)show vlan
VLAN Name Status IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1 default active 5 1/1-2
3/1-48
4/1-16
1002 fddi-default active 6
1003 token-ring-default active 9
1004 fddinet-default active 7
1005 trnet-default active 8
VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
1 enet 100001 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 trcrf 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - - - 0 0
1005 trbrf 101005 1500 - - - ibm - 0 0
VLAN DynCreated RSPAN
---- ---------- --------
1 static disabled
1002 static disabled
1003 static disabled
1004 static disabled
1005 static disabled
VLAN AREHops STEHops Backup CRF 1q VLAN
---- ------- ------- ---------- -------
1003 7 7 off
a. Ejecute el comando set vlan para crear las VLAN.
CatosSwitch> (enable)set vlanUsage: set vlan <vlan> <mod/port>
(An example of mod/port is 1/1,2/1-12,3/1-2,4/1-12)
set vlan <vlan_num> [name <name>] [type <type>] [state <state>]
[pvlan-type <pvlan_type>]
[said <said>] [mtu <mtu>]
[ring <hex_ring_number>]
[decring <decimal_ring_number>]
[bridge <bridge_number>] [parent <vlan_num>]
[mode <bridge_mode>] [stp <stp_type>]
[translation <vlan_num>] [backupcrf <off|on>]
[aremaxhop <hopcount>] [stemaxhop <hopcount>]
[rspan]

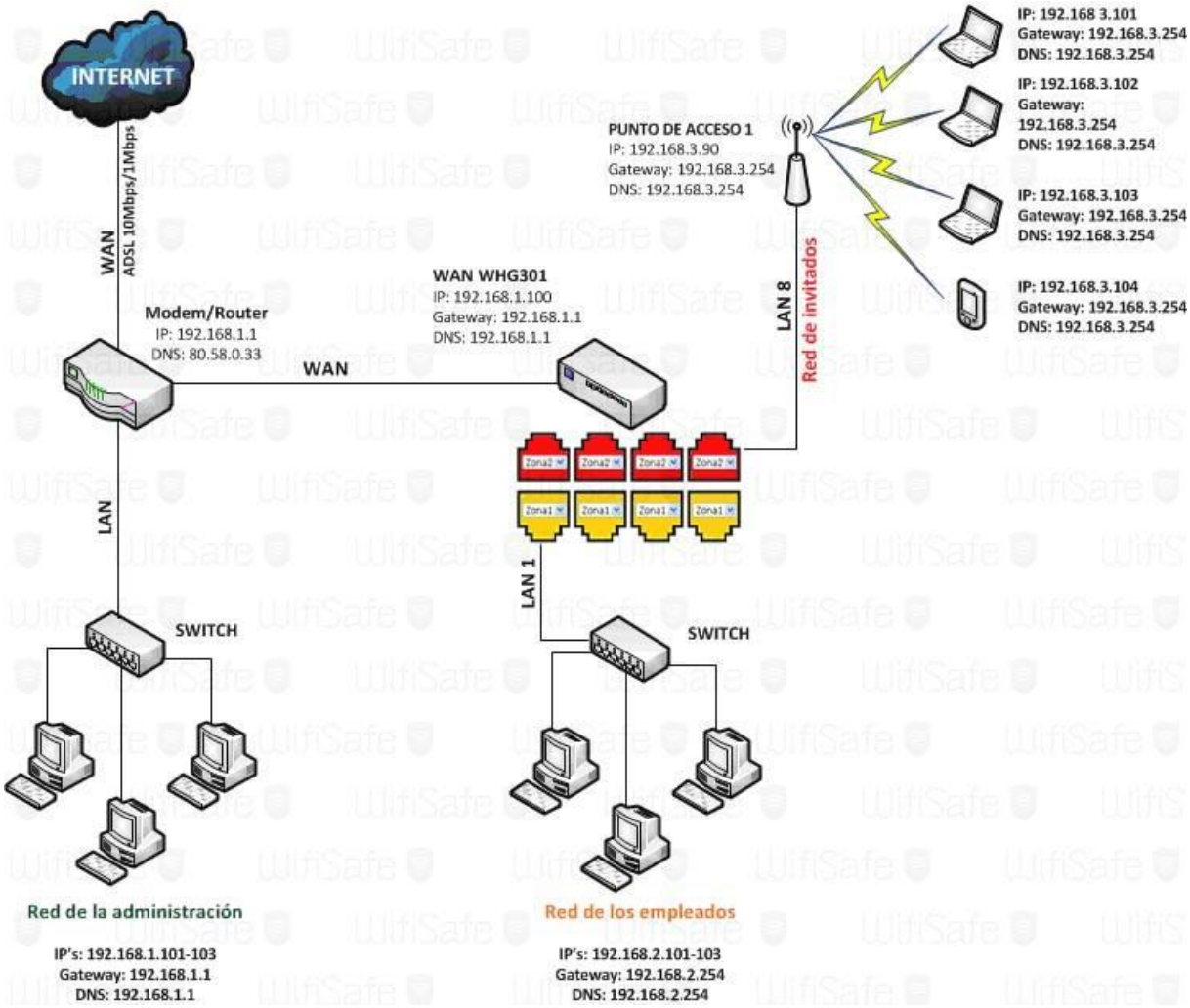
(name = 1..32 characters, state = (active, suspend)
type = (ethernet, fddi, fddinet, trcrf, trbrf)
said = 1..4294967294, mtu = 576..18190
pvlan-type = (primary,isolated,community,none)
hex_ring_number = 0x1..0xfff, decimal_ring_number = 1..4095
bridge_number = 0x1..0xf, parent = 2..1005, mode = (srt, srb)
stp = (ieee, IBM, auto), translation = 1..1005
hopcount = 1..13)
Set vlan commands:
---
set vlan Set vlan information
set vlan mapping Map an 802.1q vlan to an Ethernet vlan
CatosSwitch> (enable)set vlan 2 name cisco_vlan_2
Vlan 2 configuration successful
b. Ejecute el comando show vlan para verificar la configuración VLAN.
CatosSwitch> (enable)show vlan
VLAN Name Status IfIndex Mod/Ports, Vlans
---- --- --- --- ---
1 default active 5 1/1-2
3/1-48
4/1-16
2 cisco_vlan_2 active 75
1002 fddi-default active 6
1003 token-ring-default active 9
1004 fddinet-default active 7
1005 trnet-default active 8
VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2
---- --- --- --- --- --- --- --- --- --- ---
1 enet 100001 1500 - - - - - 0 0
2 enet 100002 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 trcrf 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - - - 0 0
1005 trbrf 101005 1500 - - - IBM - 0 0

Configurar un Hot Spot

Manual de configuración básica Hotspot

En este escenario disponemos de una línea ADSL de 10Mbps de bajada y 1Mbps de subida. La red existente se compone de un MODEM/router, un switch y tres PCs.

Es necesario conectar el puerto WAN del WHG301 a un puerto LAN del MODEM/Router, para que pueda haber conectividad con Internet. El WHG301 tendrá dos zonas de servicio. Cada una de ellas, tendrá asignados 4 puertos LAN.



Definición de las Zonas

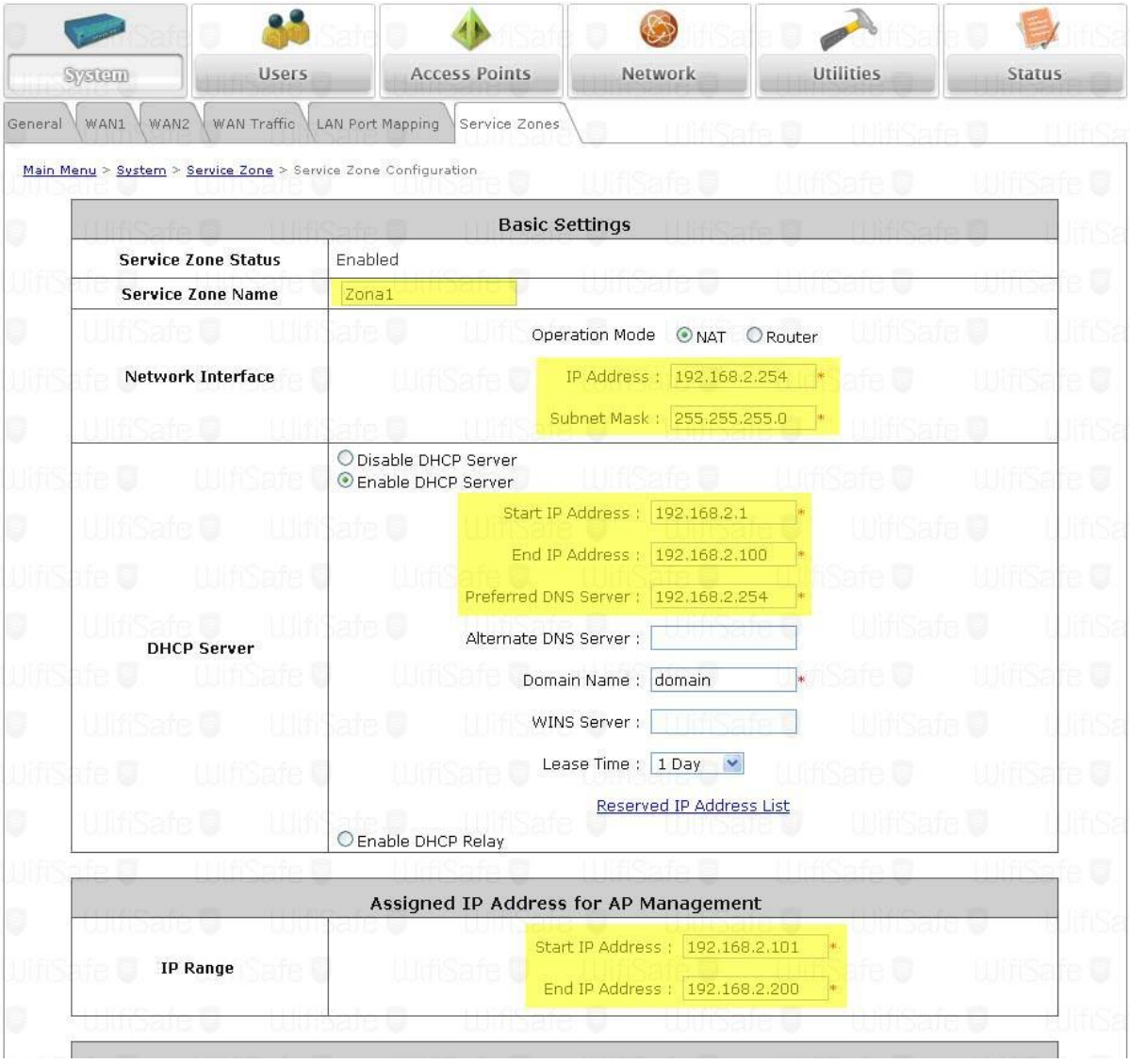
Es el punto más importante a la hora de hacer la configuración de nuestros sistema de HotSpot, se ha de hacer un análisis de los requerimientos así como la definición de políticas de uso y seguridad que se quiere dar a cada Zona, como son anchos de banda, tipo de autenticación, horas de utilización, acceso a recursos determinados, etc…

En nuestro manual, la **Zona 1** tiene asignados los puertos LAN1, LAN2, LAN3 y LAN4. Esta zona será la red de los empleados, y la autentificación se realizará usando cuentas locales, previamente generadas. Esta zona tiene asignado un límite de caudal de 2 Mbps / 56 Kbps. Además, también hay establecido un limite de uso de lunes a viernes.
La **Zona 2** tiene asignados los puertos LAN5, LAN6, LAN7 y LAN8. Esta zona será la red de invitados, y su autentificación se realizará usando cuentas on-demand, que se generarán aleatoriamente a medida que los clientes wifi las vayan solicitando al sistema.

El invitado dispondrá de 3 bonos o Billings Plans; 1 hora, 2 horas o 3 horas. Esta zona tiene asignado un límite de caudal de 2 Mbps / 56 Kbps. En esta zona no hay límite de uso horario, y los clientes podrán usar el servicio toda la semana.

Zona 1 – Red de empleados	**Zona 2 – Red de invitados**
Puertos asignados: LAN1-LAN2-LAN3-LAN4 **IP:** 192.168.2.254 **Método autenticación:** Cuentas locales **Política:** Policy 1 **Grupo:**Group 1	**Puertos asignados:**LAN5-LAN6-LAN7-LA **IP:**192.168.3.254 **Método autenticación:** Cuentas on-demand **Política:** Policy 2 **Grupo: Group 2**
Política 1	**Política 2**
Conexiones TCP concurrentes: 25 Horario de uso: De lunes a viernes	**Conexiones TCP concurrentes:** 5 **Horario de uso:** Todos los días
Grupo 1	**Grupo 2**
Total asignado: 2Mb / 256 Kbps **TDescarga máxima individual:** 256 Kbps **TCaudal garantizado:** 256 Kbps **TSubida máxima individual:** 64 Kbps **TCaudal garantizado:** 64 Kbps	**Total asignado:** 5Mb / 384 Kbps **Descarga máxima individual::** 256 Kbps **Caudal garantizado::** 256 Kbps **Subida máxima individual::** 64 Kbps **Caudal garantizado::** 64 Kbps
	Billins Plans (bonos)
	1 h --- 1 € 2 h --- 2 € 3 h --- 3 €

Creando la Zona 1



Modificamos los campos marcados en amarillo tal y como se indica en la imagen anterior. No olvidemos nombrar a la zona “Default” como “Zona 1”. Una vez hecho esto, aplicaremos cambios y nos solicitará un reinicio del sistema.

Políticas

Mediante las políticas podemos entre otras cosas, limitar la cantidad máxima de sesiones concurrentes, establecer reglas en el firewall y en qué horas y días se podrá usar el servicio, a través de un calendario de uso segmentado en horas y días de la semana.

Vamos a crear dos políticas; Policy 1 y Policy 2

Policy 1

- **Máximo de sesiones concurrentes:** 25
  Perfil de calendario *(Schedule Profile)*: Todas las horas de lunes a viernes

Policy 2

- **Máximo de sesiones concurrentes:** 5
- **Perfil de calendario *(Schedule Profile)*:** Todas las horas, durante toda la semana.

No olvidemos aplicar cambios en cada una de las políticas modificadas.

Creando Billing Plans (Tickets de servicio)

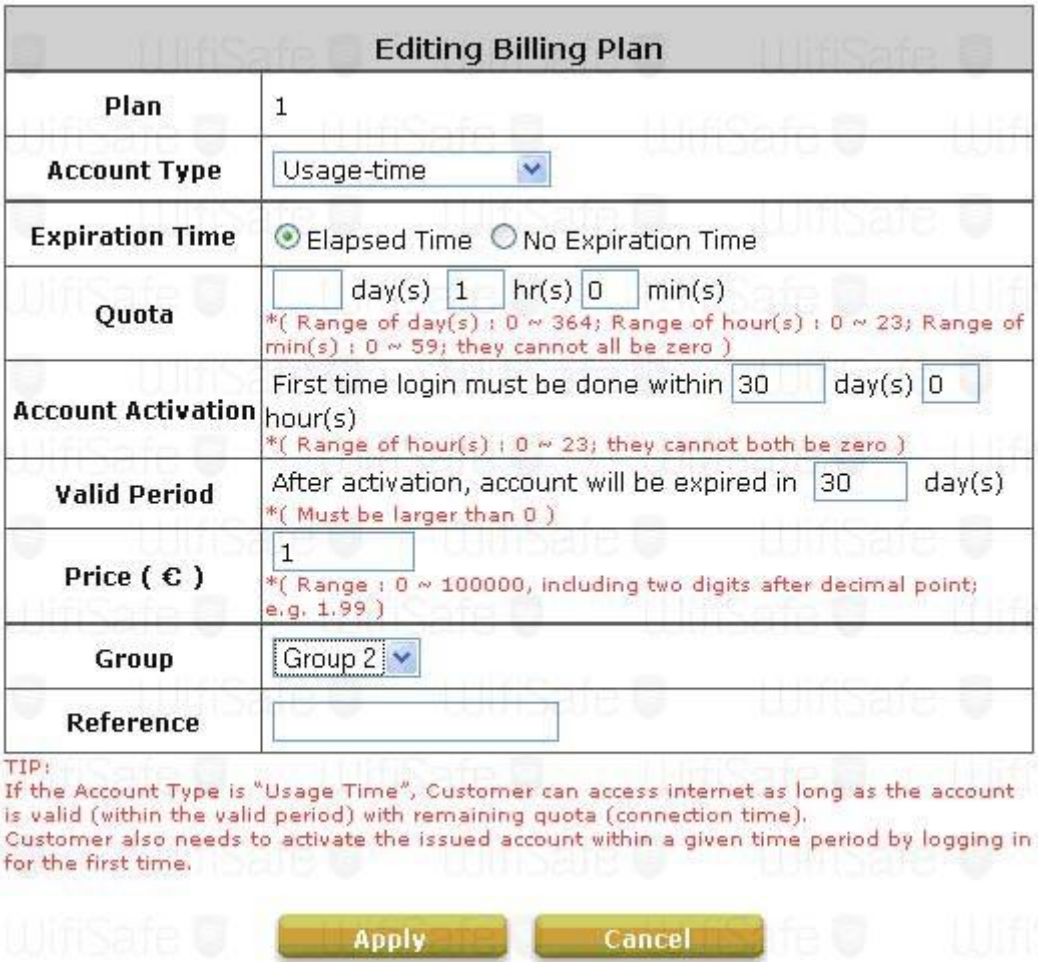
Las cuentas on demand se generarán a medida que el usuario solicite el servicio. Éstas las podemos generar desde el propio hotspot, o si lo preferimos, podemos usar el Printer Kit de 4ipnet para hacerlo de una forma más rápida y cómoda.

Al igual que las cuentas locales, las on-demand usan un prefijo para identificarse. Las cuentas se generan de la siguiente forma.

- **Usuario:** A87Bs8d@ondemand
- **Password:** bX892kJ

Si queremos podemos modificar el prefijo “ondemand”, para ello tenemos que ir a Users / Authetication / On-demand user / General Settings.

También tendremos que establecer la divisa (€uro) en caso que el servicio sea de pago. Y por último seleccionamos el grupo “Group 2”. Aplicamos cambios.



Modificando el portal cautivo

Podemos modificar algunos de los parámetros del portal cautivo integrado en el WHG301. Cada zona de servicio tiene un portal cautivo independiente. Podemos usar el portal cautivo integrado en el hotspot, o bien usar una plantilla y modificar algunos parámetros, como el color de fondo, color de fuente y página, etc… También tenemos la posibilidad de subir una página personalizada o usar una página externa, siguiendo las puntualizaciones que se encuentran en el manual del fabricante sobre la implementación y uso de páginas externas.

Para modificar el portal cautivo tenemos que ir a a cada una de las zonas de servicio en System / Service Zone / Service Zone Configuration. Elegimos la zona de servicio que queramos y buscamos en “Custom Pages”. El botón configure nos permitirá elegir la opción que más se ajuste a nuestras necesidades.

Y con esto ya tenemos el Hotspot configurado, con 2 zonas de servicio, con 2 grupos de usuarios y con 2 políticas aplicadas a estos grupos. Se pueden crear todas las zonas de servicio que necesitemos, siempre y cuando no se superen las limitaciones que tenga cada versión de HotSpot, así como combinar grupos y políticas de usuario en función de las necesidades que requiramos.